



Guía del usuario

AWS Security Hub



AWS Security Hub : Guía del usuario

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 AWS Security Hub?	1
Características	1
Integraciones	2
Regiones de AWS compatible con la vista previa pública	2
Accesibilidad	4
Precios	4
Introducción	4
Habilitación de Security Hub	5
Recomendaciones	14
Conceptos	16
Hallazgos del OCSF	17
Hallazgos de cobertura	18
Hallazgos de cobertura para Security Hub CSPM	18
Hallazgos de cobertura para GuardDuty	19
Hallazgos de cobertura para Amazon Inspector	19
Hallazgos de cobertura para Macie	20
Hallazgos de exposición	20
Recursos admitidos	20
Características compatibles	21
Generar hallazgos de exposición	22
Determinar el nivel de gravedad de un hallazgo de exposición	27
Revisar los resultados de la exposición	28
Corregir los hallazgos de exposición	30
Descubrimientos de la secuencia de ataque	92
Revisar los hallazgos de la secuencia de ataque	92
Corregir los hallazgos de la secuencia de ataques	94
Reglas de automatización	94
Mejoras clave	95
Integración externa	95
Criterios compatibles con el OCSF	95
Campos OCSF para AutomationRulesFindingFieldsUpdate	96
Integraciones de terceros	96
Cree una clave KMS	96
Jira Cloud	99

ServiceNow	104
Panel de control	107
El widget de resumen de exposiciones	108
El widget de resumen de amenazas	108
El widget de cobertura de seguridad	109
Visualización de detalles sobre los recursos en Security Hub	109
Gráfico de posibles rutas de ataque	110
Deshabilitación de Security Hub	111
¿Qué es AWS Security Hub CSPM?	112
Ventajas de Security Hub CSPM	113
Acceso a Security Hub (CSPM)	114
Servicios relacionados	115
Prueba gratuita, uso y precios de Security Hub CSPM	115
Visualización de detalles de uso y costo estimado	116
Información sobre precios	116
Conceptos de Security Hub CSPM	117
Activación de Security Hub CSPM	124
Verificación de los permisos necesarios	124
Habilitación de la integración de Security Hub CSPM con Organizations	124
Configuración centralizada	125
Activación manual del Security Hub CSPM	126
Script de habilitación de múltiples cuentas	128
Próximos pasos: gestión de la postura e integraciones	129
Configuración AWS Config para Security Hub CSPM	129
Consideraciones antes de habilitar y configurar AWS Config	130
Registrar los recursos en AWS Config	130
Formas de habilitar y configurar AWS Config	132
Control de configuración 1	133
Generación de reglas vinculadas a servicios	133
Consideraciones sobre costos	134
Configuración local	134
Configuración centralizada	135
Beneficios de usar la configuración centralizada	136
¿Cuándo se debe utilizar la configuración centralizada?	137
Términos y conceptos de la configuración centralizada	138
Habilitar la configuración centralizada	144

Administración centralizada frente a autoadministración	149
Funcionamiento de las políticas de configuración	154
Creación y asociación de políticas de configuración	160
Revisar el estado y los detalles de las políticas de configuración	166
Actualización de las políticas de configuración	170
Eliminación de políticas de configuración	175
Desasociación de una configuración	177
Configuración en contexto	179
Deshabilitación de la configuración centralizada	181
Administración de Security Hub (CSPM) para varias cuentas	185
Administrar cuentas con AWS Organizations	185
Administración manual de cuentas mediante invitación	186
Recomendaciones para entornos de varias cuentas	187
Número máximo de cuentas miembro	187
Creación de relaciones administrador-miembro	187
Coordinar cuentas de administrador en todos los servicios	188
Administrar cuentas con AWS Organizations	189
Integración con AWS Organizations	191
Activación automática de Security Hub CSPM en cuentas nuevas	199
Activación manual de Security Hub CSPM en cuentas nuevas	202
Desasociación de cuentas de la organización como cuentas de miembro	204
Administración de cuentas por invitación	206
Agregar e invitar cuentas de miembro	208
Cómo responder a una invitación	212
Desasociación de cuentas miembro	215
Eliminación de cuentas de miembro	216
Desvinculación de una cuenta de administrador	218
¿Está haciendo la transición a AWS Organizations	220
Acciones permitidas en las cuentas de administrador y de miembro	221
Efecto de las acciones de la cuenta en los datos del CSPM	228
Security Hub (CSPM) desactivado	228
Cuenta miembro disociada de la cuenta de administrador	229
Cómo eliminar una cuenta miembro de una organización	229
Cuenta suspendida	230
Cuenta cerrada	230
Agregación de datos del CSPM en todas las regiones	232

Tipos de datos que se agregan	233
Agregación de cuentas de administrador y de miembros	235
Configuración centralizada y agregación	236
Habilitación de agregación	237
Revisión de la configuración de agregación	239
Actualización de la configuración de agregación	241
Detención de la agregación	243
Para eliminar el agregador de resultados (consola)	243
Estándares CSPM	245
Referencia de estándares	246
AWS Mejores prácticas de seguridad fundamentales	248
AWS Etiquetado de recursos	266
Punto de referencia sobre fundaciones CIS AWS	273
NIST SP 800-53, revisión 5	291
NIST SP 800-171, revisión 2	310
PCI DSS	316
Estándar de gestión de servicios	327
Habilitación de un estándar	342
Habilitar un estándar en varias cuentas y Regiones de AWS	343
Habilitar un estándar en una sola cuenta y Región de AWS	344
Comprobar el estado de un estándar	346
Revisar los detalles de un estándar	349
Descripción de la puntuación de seguridad del estándar	349
Revisar los controles para determinar si existe una norma	350
Desactivar los estándares con habilitación automática	352
Desactivación de un estándar	354
Deshabilitar un estándar en varias cuentas y Regiones de AWS	354
Deshabilitar un estándar en una sola cuenta y Región de AWS	355
Controles CSPM	358
Vista de controles consolidados	358
Puntuación general de seguridad de los controles	359
Referencia de controles	360
Registro de cambios para los controles	499
Cuenta de AWS controles	576
AWS Amplify controles	577
Controles de Amazon API Gateway	580

AWS AppConfig controles	587
AppFlow Controles de Amazon	593
AWS App Runner controles	595
AWS AppSync controles	598
Controles de Amazon Athena	603
AWS Backup controles	608
AWS Batch controles	617
AWS Certificate Manager controles	623
AWS CloudFormation controles	627
CloudFront Controles de Amazon	630
AWS CloudTrail controles	640
CloudWatch Controles de Amazon	652
AWS CodeArtifact controles	700
AWS CodeBuild controles	701
Controles de Amazon CodeGuru Profiler	707
Controles de Amazon CodeGuru Reviewer	709
Controles de Amazon Cognito	711
AWS Config controles	712
Controles de Amazon Connect	715
Controles de Amazon Data Firehose	718
AWS DataSync controles	719
Controles de Amazon Detective	721
AWS DMS controles	723
Controles de Amazon DocumentDB	737
Controles de Amazon DynamoDB	743
EC2 Controles de Amazon	751
Controles EC2 de Amazon Auto Scaling	831
Controles de Amazon ECR	839
Controles de Amazon ECS	845
Controles de Amazon EFS	860
Controles de Amazon EKS	867
ElastiCache Controles de Amazon	874
AWS Elastic Beanstalk controles	880
Controles del equilibrador de carga elástico	884
Controles de Elasticsearch	899
Controles de Amazon EMR	908

EventBridge Controles de Amazon	912
Controles de Amazon Fraud Detector	916
FSx Controles de Amazon	924
AWS Global Accelerator controles	929
AWS Glue controles	931
GuardDuty Controles de Amazon	934
AWS Identity and Access Management controles	949
Controles de Amazon Inspector	987
AWS IoT controles	992
AWS Controles de IoT Events	1001
AWS SiteWise Controles de IoT	1006
AWS TwinMaker Controles de IoT	1014
AWS Controles IoT Wireless	1021
Controles de Amazon IVS	1026
Controles de Amazon Keyspaces	1031
Amazon Kinesis Kinesis Kinesis Controles	1033
AWS KMS controles	1037
AWS Lambda controles	1042
Controles de Amazon Macie	1049
Controles de Amazon MSK	1051
Controles de Amazon MQ	1053
Controles de Amazon Neptune	1059
AWS Network Firewall controles	1067
Controles OpenSearch de Amazon Service	1077
AWS Private CA controles	1087
Controles de Amazon RDS	1090
Controles de Amazon Redshift	1137
Controles de Amazon Redshift sin servidor	1155
Controles de Amazon Route 53	1163
Controles de Amazon S3	1165
Controles de Amazon SageMaker AI	1190
AWS Secrets Manager controles	1199
AWS Service Catalog controles	1205
Controles para Amazon Simple Email Service	1206
Controles de Amazon SNS	1210
Controles de Amazon SQS	1215

AWS Step Functions controles	1218
AWS Systems Manager controles	1221
AWS Transfer Family controles	1227
AWS WAF controles	1237
WorkSpaces Controles de Amazon	1245
Permisos para configurar los controles	1246
Habilitación de controles	1247
Habilitación de un control en todos los estándares	1248
Habilitación de un control en un estándar específico	1251
Habilitación automática de nuevos controles	1254
Deshabilitación de controles	1256
Deshabilitar un control en todos los estándares	1257
Deshabilitación de un control en un estándar específico	1260
Controles sugeridos para deshabilitar	1263
Controles y puntuaciones de seguridad	1268
AWS Config Recursos necesarios para los hallazgos de control	1269
Programación para ejecutar comprobaciones de seguridad	1320
Generación y actualización de los resultados de control	1322
Estado de conformidad y el estado de control	1337
Calcular las puntuaciones de seguridad	1339
Categorías de control	1342
Identificar	1343
Protección	1344
Detect	1345
Respuesta	1345
Recuperar	1346
Revisar los detalles de los controles	1346
Visualización de detalles de un control	1347
Controles de filtrado y clasificación	1349
Parámetros de control	1350
Efecto de la modificación de los valores de parámetros de control	1351
Controles que admiten parámetros personalizados	1353
Revisión de los valores actuales de los parámetros de control	1353
Personalización de parámetros de control	1356
Reversión de los parámetros de control predeterminados	1361
Comprobación del estado de los cambios de los parámetros de control	1365

Revisión y gestión de los hallazgos de control	1366
Filtrado y clasificación de resultados de control	1367
Muestras de los hallazgos de los controles	1367
Integraciones de CSPM	1393
Revisar una lista de integraciones	1393
Habilitación del flujo de resultados desde una integración	1395
Deshabilitación del flujo de resultados desde una integración	1396
Visualizar resultados desde una integración	1397
Servicio de AWS integraciones	1398
Descripción general de las integraciones de AWS servicios con Security Hub (CSPM)	1399
AWS servicios que envían los resultados a Security Hub (CSPM)	1400
AWS servicios que reciben las conclusiones de Security Hub (CSPM)	1417
Integraciones de terceros	1420
Descripción general de las integraciones de terceros con Security Hub CSPM	1421
Integraciones de terceros que envían los resultados a Security Hub (CSPM)	1430
Integraciones de terceros que reciben las conclusiones de Security Hub (CSPM)	1447
Integraciones de terceros que envían y reciben las conclusiones de Security Hub (CSPM)	1454
Integraciones de productos personalizados	1456
Requisitos y recomendaciones para las integraciones de productos personalizados	1456
Actualización de los resultados de los productos personalizados	1457
Integraciones personalizadas de ejemplo	1457
Hallazgos del CSPM	1459
BatchImportFindings para encontrar proveedores	1461
Requisitos previos para utilizar BatchImportFindings	1461
Determinación de si se debe crear o actualizar un hallazgo	1461
Restricciones para la actualización de resultados con BatchImportFindings	1462
Actualizar los resultados mediante FindingProviderFields	1462
BatchUpdateFindings para clientes	1464
Campos disponibles para BatchUpdateFindings	1465
Configuración del acceso a BatchUpdateFindings	1465
Revisión de los detalles y el historial de resultados	1468
Revisión de los detalles y el historial de resultados	1470
Filtrado de resultados	1473
Filtros predeterminados en las listas de búsqueda	1473
Instrucciones para añadir filtros	1474
Agrupación de hallazgos	1476

Configuración del estado de flujo de trabajo de los resultados	1477
Configuración del estado de flujo de trabajo de los resultados	1478
Envío de hallazgos a una acción personalizada	1480
Formato de búsqueda: ASFF	1481
ASFF y consolidación	1561
Atributos de nivel superior necesarios del ASFF	1624
Atributos de nivel superior opcionales del ASFF	1635
Objeto Resources del ASFF	1657
Información sobre el CSPM	1782
Revisar los conocimientos y actuar en función de ellos	1783
Visualización y adopción de medidas sobre los resultados de la información	1783
Para visualizar y tomar medidas sobre los hallazgos en los resultados de la información (console)	1785
Conocimientos administrados	1786
Información personalizada	1797
Creación de hallazgos personalizados	1798
Edición de hallazgos personalizados	1801
Eliminación de hallazgos personalizados	1803
Automatizaciones de CSPM	1806
Reglas de automatización	1807
Definición de criterios de regla y acciones de regla	1807
Criterios de regla y acciones de regla disponibles	1808
Resultados que las reglas de automatización evalúan	1814
Cómo funciona el orden de las reglas	1815
Creación de reglas de automatización	1816
Visualización de las reglas de automatización	1820
Edición de reglas de automatización	1821
Edición del orden de las reglas	1823
Eliminación o desactivación de las reglas de automatización	1825
Ejemplos de reglas de automatización	1826
Respuesta y corrección automatizadas	1833
EventBridge tipos de eventos	1835
EventBridge formatos de eventos	1837
Configuración de una regla EventBridge	1839
Configuración y uso de acciones personalizadas	1845
Panel de control de CSPM	1851

El widget de resumen de riesgos	1851
El widget de resumen de amenazas	1851
El widget de cobertura de seguridad	1852
Widgets disponibles para el panel Resumen	1852
Widgets mostrados de forma predeterminada	1852
Widgets ocultos de forma predeterminada	1855
Filtrado del panel Resumen	1856
Creación y almacenamiento de conjuntos de filtros	1857
Actualización o eliminación de conjuntos de filtros	1857
Personalización del panel Resumen	1858
Límites regionales de CSPM	1860
Restricciones de agregación entre regiones	1860
Disponibilidad de las integraciones por región	1860
Integraciones compatibles en las regiones de China (Pekín) y China (Ningxia)	1860
Integraciones compatibles en las regiones (EE. UU. este) y AWS GovCloud AWS GovCloud (EE. UU., oeste)	1861
Disponibilidad de los estándares por región	1863
Disponibilidad de los controles por región	1863
Límites regionales de los controles del CSPM	1863
Este de EE. UU. (Norte de Virginia)	1865
Este de EE. UU. (Ohio)	1865
Oeste de EE. UU. (Norte de California)	1867
Oeste de EE. UU. (Oregón)	1870
África (Ciudad del Cabo)	1871
Asia-Pacífico (Hong Kong)	1875
Asia-Pacífico (Hyderabad)	1878
Asia-Pacífico (Yakarta)	1886
Asia-Pacífico (Malasia)	1893
Asia-Pacífico (Melbourne)	1909
Asia-Pacífico (Bombay)	1919
Asia-Pacífico (Osaka)	1920
Asia-Pacífico (Seúl)	1926
Asia-Pacífico (Singapur)	1927
Asia-Pacífico (Sídney)	1929
Asia-Pacífico (Tailandia)	1930
Asia-Pacífico (Tokio)	1948

Canadá (centro)	1950
Oeste de Canadá (Calgary)	1952
China (Pekín)	1967
China (Ningxia)	1977
Europa (Fráncfort)	1987
Europa (Irlanda)	1988
Europa (Londres)	1989
Europa (Milán)	1991
Europa (París)	1996
Europa (España)	1998
Europa (Estocolmo)	2006
Europa (Zúrich)	2009
Israel (Tel Aviv)	2017
México (central)	2027
Medio Oriente (Baréin)	2046
Medio Oriente (EAU)	2050
América del Sur (São Paulo)	2058
AWS GovCloud (Este de EE. UU.)	2060
AWS GovCloud (EEUU-Oeste)	2071
Crear recursos de CSPM con CloudFormation	2082
Security Hub, CSPM y plantillas AWS CloudFormation	2082
Más información sobre AWS CloudFormation	2083
Suscribirse a los anuncios del CSPM	2084
Formato de los mensajes de Amazon SNS	2090
Desactivación de Security Hub CSPM	2092
Seguridad	2095
Protección de los datos	2096
Identity and Access Management	2097
Público	2097
Autenticación con identidades	2098
Administración de acceso mediante políticas	2102
Cómo funciona Security Hub con IAM	2104
Ejemplos de políticas basadas en identidades	2113
Roles vinculados a servicios	2119
AWS políticas gestionadas	2122
Solución de problemas	2140

Validación de conformidad	2144
Resiliencia	2145
Seguridad de la infraestructura	2145
Puntos de conexión de VPC (AWS PrivateLink)	2146
Consideraciones para los puntos de conexión de VPC de Security Hub	2146
Creación de un punto de conexión de VPC de la interfaz para Security Hub	2147
Creación de una política de punto de conexión de VPC para Security Hub	2147
Subredes compartidas	2148
Registro de llamadas a la API	2149
Información sobre CSPM de Security Hub en CloudTrail	2149
Ejemplo: entradas del archivo de registro CSPM de Security Hub	2150
Etiquetado de recursos	2152
Conceptos básicos del etiquetado	2152
Uso de etiquetas en políticas de IAM	2154
Agregar etiquetas.	2155
Edición de etiquetas para recursos	2158
Revisión de las etiquetas	2160
Eliminación de etiquetas	2162
Cuotas	2165
Cuotas máximas	2165
Cuotas de tarifas	2165
Historial de documentos	2166
.....	mmcclxxvi

¿Qué es AWS Security Hub?

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

AWS Security Hub es una solución de seguridad en la nube unificada que prioriza sus problemas de seguridad críticos y le ayuda a responder a escala. Security Hub detecta los problemas de seguridad al correlacionar y enriquecer automáticamente las señales de seguridad de múltiples fuentes, como la gestión de la postura, la gestión de vulnerabilidades (Amazon Inspector), los datos confidenciales (Macie) y la detección de amenazas (GuardDuty). Esto permite a los equipos de seguridad priorizar los riesgos activos en sus entornos de nube mediante análisis automatizados e información contextual. Mediante visualizaciones intuitivas, Security Hub transforma las señales de seguridad complejas en información procesable, lo que le permite tomar decisiones informadas sobre su seguridad rápidamente. Security Hub también incluye flujos de trabajo de respuesta automatizados para ayudarlo a remediar los riesgos, mejorar la productividad del equipo y minimizar las interrupciones operativas.

Características

Solución de seguridad unificada

Obtenga una visibilidad más amplia en todo su entorno de nube mediante la administración centralizada en una solución de seguridad en la nube unificada.

Información de seguridad procesable

Obtenga información útil sobre seguridad mediante análisis avanzados para obtener información sobre los riesgos de seguridad asociados a su entorno.

Tiempos de respuesta reducidos

Optimice los tiempos de respuesta con flujos de trabajo automatizados y un sistema de venta de entradas integrado.

Hallazgos de exposición

Security Hub correlaciona los resultados de las comprobaciones de control del CSPM de Security Hub, Amazon Inspector y otros Servicios de AWS para detectar las exposiciones asociadas a los recursos. AWS

Los hallazgos están formateados en el marco del esquema de ciberseguridad abierto (OCSF)

Security Hub genera hallazgos en OCSF y recibe hallazgos en OCSF de Security Hub CSPM y otros: Servicios de AWS

- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector

Panel de control

La consola Security Hub ofrece una vista completa de las exposiciones, las amenazas, la cobertura de seguridad y los recursos, así como una visualización interactiva denominada gráfico de la ruta de ataque, que muestra cómo los posibles atacantes pueden acceder a los recursos asociados a una detección de exposición y tomar el control de ellos.

Integraciones con productos de terceros

Puede mejorar su postura de seguridad con las integraciones de Security Hub. Por ejemplo, si usa Jira Cloud o ServiceNow ITSM puede usar esta función para crear tickets a partir de los hallazgos.

Integraciones

Security Hub se integra con lo siguiente Servicios de AWS.

- AWS Security Hub Cloud Security Posture Management (CSPM)
- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie

Regiones de AWS compatible con la vista previa pública

Security Hub admite lo siguiente Regiones de AWS en esta versión preliminar pública.

- Asia-Pacífico (Tokio)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Osaka)
- Asia-Pacífico (Mumbai)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Canadá (centro)
- Europa (Fráncfort)
- Europa (Estocolmo)
- Europa (Irlanda)
- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)
- Europa (Londres)
- Europa (París)
- América del Sur (São Paulo)
- Este de EE. UU. (Norte de Virginia)
- Este de EE. UU. (Ohio)

Las siguientes son opciones opcionales Regiones de AWS, que requieren que las habilites antes de poder acceder a ellas.

- Africa (Cape Town)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Yakarta)
- Europa (Milán)
- Middle East (Bahrain)

Para obtener información al respecto Regiones de AWS, consulte el [estado de la suscripción](#) en la Guía del usuario Regiones de AWS y las zonas de disponibilidad.

Accesibilidad

Security Hub está disponible en la Regiones de AWS lista anterior. Puede habilitar Security Hub para cuentas individuales o cuentas de su organización. Puede acceder a Security Hub de la siguiente manera:

Consola de Security Hub

La consola Security Hub es una interfaz basada en un navegador que puede utilizar para crear y administrar AWS recursos. En esta consola, puede acceder a su cuenta, sus datos y sus recursos.

API de Security Hub

La API de Security Hub le brinda acceso programático a su cuenta, datos y recursos. Puede enviar solicitudes HTTPS directamente a Security Hub.

AWS CLI

Con [el AWS CLI](#), puede ejecutar comandos en la línea de comandos del sistema para realizar tareas y crear scripts que realicen tareas. En algunos casos, AWS CLI puede resultar más útil que la consola de Security Hub.

AWS SDKs

[AWS SDKs](#) constan de bibliotecas y código de muestra para varios lenguajes de programación y plataformas (C++, Go, Java, .NET y Python). Proporcionan acceso programático a Security Hub y a otros Servicios de AWS en el idioma que prefiera y pueden ayudarle a gestionar tareas como la gestión de errores, la firma de solicitudes y el reintento de las solicitudes.

Precios

El uso de Security Hub no tiene ningún coste. Security Hub es gratuito durante esta versión preliminar pública.

Primeros pasos con Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

En los temas de esta sección se describe cómo empezar a utilizar Security Hub.

Habilitación de Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Puede activar Security Hub para cualquiera Cuenta de AWS. Los procedimientos de este tema describen cómo habilitar Security Hub desde una cuenta de administración de AWS la organización, una cuenta de administrador delegado y una cuenta independiente.

Note

Después de activar Security Hub, las exposiciones en su entorno se analizan inmediatamente. Sin embargo, puede esperar hasta 6 horas para recibir una evaluación de la exposición de un recurso.

Habilitar Security Hub para una organización

El procedimiento de esta sección describe cómo habilitar Security Hub para la cuenta de administración de la AWS organización. El procedimiento supone que ha configurado un administrador delegado para Security Hub CSPM e incluye un paso en el que puede configurar un administrador delegado para su organización en Security Hub. Para obtener más información sobre cómo configurar un administrador delegado en Security Hub, consulte [Configurar una cuenta de administrador delegado en Security Hub](#).

Si decide configurar un administrador delegado para Security Hub durante la activación, tendrá que [crear una política de recursos en la AWS Organizations consola que permita al](#) administrador delegado realizar acciones en nombre de su organización. Puede utilizar el siguiente ejemplo de política de recursos para la cuenta de administrador delegado.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement",
      "Effect": "Allow",
```

```
"Principal": {
  "AWS": "arn:aws:iam::delegated-administrator-account-id:root"
},
"Action": [
  "organizations:AttachPolicy",
  "organizations:CreatePolicy",
  "organizations:DetachPolicy",
  "organizations>DeletePolicy",
  "organizations:UpdatePolicy",
  "organizations:ListPolicies",
  "organizations:ListPoliciesForTarget",
  "organizations:ListTargetsForPolicy",
  "organizations:DescribePolicy",
  "organizations:DescribeEffectivePolicy",
  "organizations:DisablePolicyType",
  "organizations:EnablePolicyType"
],
"Resource": "*"
}
]
```

Si no configura un administrador delegado, puede hacerlo más adelante. Para obtener más información, consulte [Configurar una cuenta de administrador delegado en Security Hub](#). El tema incluye un procedimiento que describe cómo configurar un administrador delegado para su organización desde la página General de la consola de Security Hub.

El siguiente procedimiento describe cómo configurar una cuenta de administrador delegado para su organización en Security Hub.

Para habilitar Security Hub en una cuenta de administración de la AWS organización

1. Inicie sesión en su AWS cuenta con las credenciales de la cuenta de administración de su AWS organización. Abra la consola de Security Hub en la [https://console.aws.amazon.com/securityhub/versión 2/home](https://console.aws.amazon.com/securityhub/versión%20/home).
2. En la página de inicio de Security Hub, selecciona Security Hub. Elija Comenzar.
3. (Opcional) Para la cuenta de administrador delegado, configure un administrador delegado en función de las opciones ofrecidas. Como práctica recomendada, recomendamos utilizar el mismo administrador delegado en todos los servicios de seguridad para lograr una gobernanza coherente. Para obtener más información sobre cómo configurar una cuenta de administrador delegado, consulte [Configurar una cuenta de administrador delegado en Security Hub](#).

4. (Opcional) Para habilitar la cuenta, selecciona la casilla para habilitar Security Hub en tu AWS cuenta.
5. Selecciona Copiar y adjuntar para abrir la configuración de la organización. En la consola de Organizations, seleccione Delegar en Administrador delegado de AWS Organizations y pegue la política de recursos. Seleccione Crear política.
6. Ve a la consola de Security Hub. Elija Configurar.

Al habilitar Security Hub, se crea un rol vinculado a un servicio denominado [AWSServiceRoleForSecurityHubV2](#) en su cuenta y se agrega una grabadora vinculada al servicio a su cuenta. Una grabadora vinculada a un servicio es un tipo de AWS Config grabadora gestionada por un AWS servicio que puede registrar los datos de configuración de los recursos específicos del servicio. Con un grabador vinculado a un servicio, Security Hub permite un enfoque basado en eventos para obtener los elementos de configuración de recursos necesarios para la cobertura del análisis de exposición. Un grabador vinculado a un servicio se configura por separado. Cuenta de AWS Región de AWS

 Note

Si configuras un administrador delegado, el administrador delegado puede crear y aplicar una política que le permita habilitar y deshabilitar las cuentas de los miembros de Security Hub. Para obtener más información, consulte [Crear una política como administrador delegado para administrar las cuentas de los miembros](#).

Habilitar Security Hub para el administrador delegado

Si la cuenta de administración de la AWS organización establece un administrador delegado para su organización, el administrador delegado debe habilitar Security Hub para su cuenta. El administrador delegado debe completar el siguiente procedimiento, pero solo si no ha habilitado Security Hub para su cuenta. Para obtener información sobre cómo configurar un administrador delegado, consulte [Configurar una cuenta de administrador delegado en Security Hub](#).

Para habilitar Security Hub para una cuenta de administrador delegado

1. Inicie sesión en su AWS cuenta con sus credenciales de administrador delegadas y abra la consola de Security Hub en la <https://console.aws.amazon.com/securityhub/v2/home>.
2. En la página de inicio de Security Hub, selecciona Security Hub y elige Comenzar.

3. Seleccione **Habilitar**.
4. (Opcional) En el caso de las etiquetas, determine si desea añadir un par clave-valor a la configuración de la cuenta.
5. Seleccione **Ir a Security Hub**.

Al habilitar Security Hub, se crea un rol vinculado a un servicio denominado [AWSServiceRoleForSecurityHubV2](#) en su cuenta y se agrega una grabadora vinculada al servicio a su cuenta. Una grabadora vinculada a un servicio es un tipo de AWS Config grabadora gestionada por un AWS servicio que puede registrar los datos de configuración de los recursos específicos del servicio. Con un grabador vinculado a un servicio, Security Hub permite un enfoque basado en eventos para obtener los elementos de configuración de recursos necesarios para la cobertura del análisis de exposición. Un grabador vinculado a un servicio se configura por separado. Cuenta de AWS Región de AWS

 Note

Como administrador delegado de una organización, puedes crear y aplicar una política que te permita habilitar y deshabilitar las cuentas de los miembros de Security Hub. Para obtener más información, consulte [Crear una política como administrador delegado para administrar las cuentas de los miembros](#).

Habilitar Security Hub para una cuenta independiente

El siguiente procedimiento describe cómo habilitar Security Hub para una cuenta independiente. Hay dos tipos de cuentas independientes que pueden habilitar Security Hub: las que Cuenta de AWS no están dentro de una organización y las que están Cuenta de AWS dentro de una organización. Una parte Cuenta de AWS interna de una AWS organización puede ser aquella en la Cuenta de AWS que un administrador delegado vincula una AWS Organizations política a la. Cuenta de AWS Para obtener más información, consulte [las políticas de Security Hub](#) en la Guía del AWS Organizations usuario.

Para habilitar Security Hub para una cuenta independiente

1. Inicie sesión en su AWS cuenta con sus credenciales y abra la consola de Security Hub en la <https://console.aws.amazon.com/securityhub/versión 2/home>.
2. En la página de inicio de Security Hub, selecciona Security Hub y elige **Comenzar**.

3. Seleccione Habilitar.

Al habilitar Security Hub, se crea un rol vinculado a un servicio denominado [AWSServiceRoleForSecurityHubV2](#) en su cuenta y se agrega una grabadora vinculada al servicio a su cuenta. Una grabadora vinculada a un servicio es un tipo de AWS Config grabadora gestionada por un AWS servicio que puede registrar los datos de configuración de los recursos específicos del servicio. Con un grabador vinculado a un servicio, Security Hub permite un enfoque basado en eventos para obtener los elementos de configuración de recursos necesarios para la cobertura del análisis de exposición. Un grabador vinculado a un servicio se configura por separado. Cuenta de AWS Región de AWS

Configuración de una cuenta de administrador delegado en Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Desde la cuenta de administración de la AWS organización, puede configurar un administrador delegado para su organización. Como práctica recomendada, recomendamos utilizar el mismo administrador delegado en todos los servicios de seguridad para lograr una gobernanza coherente. Los procedimientos de esta sección describen cómo configurar un administrador delegado para su organización de dos maneras. La primera es para una cuenta de administración de AWS la organización que no haya configurado un administrador delegado en Security Hub CSPM. La segunda forma es para una cuenta de administración de AWS la organización que habilitó Security Hub, pero omitió la configuración de un administrador delegado durante la activación.

Consideraciones

Es posible que se dé una situación en la que desee configurar un administrador delegado para Security Hub diferente del administrador delegado para Security Hub CSPM. Si tiene un administrador delegado configurado en Security Hub CSPM, tenga en cuenta lo siguiente:

- Si la cuenta de administración de la AWS organización está configurada como la administradora delegada de Security Hub CSPM, no podrá configurar esta cuenta como la administradora delegada de Security Hub. Sin embargo, puede designar a otro Cuenta de AWS miembro de la organización como administrador delegado de Security Hub. Para una gobernanza coherente de todos los servicios de seguridad, recomendamos utilizar la misma cuenta (distinta de la cuenta de

administración de la AWS organización) que el administrador delegado de Security Hub CSPM y Security Hub.

- Si una cuenta distinta de la cuenta de administración de la AWS organización está configurada como la administradora delegada de Security Hub CSPM, esta cuenta se convierte automáticamente en la administradora delegada de Security Hub. En este escenario, Security Hub solo permite Cuenta de AWS que este específico actúe como administrador delegado.

Note

Si utilizas una cuenta distinta de la cuenta de administración de la organización como administrador delegado de CSPM de Security Hub, si la eliminas a través de la consola CSPM de Security Hub o de la API de AWS Organizations, también se eliminará de Security Hub. Del mismo modo, si eliminas al administrador delegado de Security Hub mediante la consola de Security Hub o la API de AWS Organizations, se eliminará del CSPM de Security Hub. Cuando el administrador delegado se retire del Security Hub CSPM, Central Configuration se excluirá automáticamente.

El siguiente procedimiento supone que no ha establecido un administrador delegado para Security Hub CSPM y está configurando un administrador delegado para Security Hub.

Para configurar un administrador delegado en Security Hub

1. Inicie sesión en su AWS cuenta con las credenciales de la cuenta de administración de su organización y abra la consola de Security Hub en la <https://console.aws.amazon.com/securityhub/versión 2/home>.
2. En la página de inicio de Security Hub, selecciona Security Hub y elige Comenzar.
3. En Administrador delegado, selecciona Configurar. En la ventana emergente, introduzca el Cuenta de AWS número de 12 dígitos Cuenta de AWS que desee o elija una cuenta sugerida (si utiliza administradores delegados en otros servicios de seguridad) para convertirla en administrador delegado de su organización. Seleccione Save.
4. (Opcional) Para habilitar la cuenta, selecciona la casilla para habilitar Security Hub para tu. Cuenta de AWS
5. Selecciona Copiar y adjuntar para abrir la configuración de la organización. En la consola de Organizations, seleccione Delegar en Administrador delegado de AWS Organizations y pegue la política de recursos. Seleccione Crear política.

6. Ve a la consola de Security Hub. Elija Configurar.

Note

Después de configurar el administrador delegado, esa cuenta debe [habilitar Security Hub](#) y configurar políticas para recibir las conclusiones de su cuenta de miembro.

El siguiente procedimiento supone que ha activado Security Hub, pero ha omitido la configuración de un administrador delegado durante la activación. Puede configurar un administrador delegado en la consola de Security Hub desde la página General.

Para configurar un administrador delegado en la consola de Security Hub desde la página General

1. Inicie sesión en su AWS cuenta con las credenciales de la cuenta de administración de su organización y abra la consola de Security Hub en la <https://console.aws.amazon.com/securityhub/versión 2/home>.
2. En el panel de navegación, selecciona General.
3. En Administrador delegado, elija Configurar. En la ventana emergente, introduzca el Cuenta de AWS número de 12 dígitos del Cuenta de AWS que desee establecer como administrador delegado de su organización. O elige una sugerencia Cuenta de AWS si configuras un administrador delegado en otros AWS servicios de seguridad. Seleccione Save.

Tras completar este procedimiento, tendrá que copiar la declaración de política de delegación de Security Hub y adjuntarla al administrador delegado de la AWS Organizations política, de modo que el administrador delegado de Security Hub pueda realizar acciones en Security Hub. Sin esta declaración de política, el administrador delegado no puede configurar Security Hub para su organización. Para obtener más información, consulte [Adjuntar la declaración de política de delegación de Security Hub](#).

Adjunta la declaración de política de delegación de Security Hub

Desde la cuenta de administración de la organización, debe copiar la declaración de política de delegación de Security Hub y adjuntarla al administrador delegado de la AWS Organizations política, de modo que el administrador delegado de Security Hub pueda realizar acciones en Security Hub. Sin esta declaración de política, el administrador delegado no puede configurar Security Hub para su organización. Puede copiar esta política desde la página General de la consola de Security Hub.

Al hacerlo, se le dirigirá a la página de configuración de la AWS Organizations consola, donde podrá editar su administrador delegado para la AWS Organizations política. En este tema se describe cómo copiar la política en Security Hub. Para obtener información sobre cómo actualizar la política del administrador delegado, consulte [Actualizar una AWS Organizations política de delegación basada en recursos en la Guía](#) del AWS OrganizationsAWS Organizations usuario.

Para adjuntar la declaración de política de delegación de Security Hub

1. Inicie sesión en su AWS cuenta con las credenciales de la cuenta de administración de su organización y abra la consola de Security Hub en la <https://console.aws.amazon.com/securityhub/versión 2/home>.
2. En el panel de navegación, selecciona General.
3. En la declaración de política de delegación de Security Hub, seleccione Copiar y adjuntar. Accederá a la página de configuración, AWS Organizations donde podrá editar el administrador delegado para que la AWS Organizations política incluya la declaración de política de delegación. Si desea ver la declaración de política antes de copiarla, seleccione Detalles de la política.

 Note

Si configuras un administrador delegado, el administrador delegado puede crear y aplicar una política que le permita habilitar y deshabilitar las cuentas de los miembros. El procedimiento del tema siguiente describe cómo configurar esta política.

Crear una política como administrador delegado para administrar las cuentas de los miembros

Como administrador delegado de una organización, puede crear y aplicar una política que le permita habilitar y deshabilitar las cuentas de los miembros. Puede acceder a todas las políticas configuradas desde la pantalla de configuraciones de la consola de Security Hub. El siguiente procedimiento describe cómo crear esta política.

 Note

El paso 6 es un paso opcional en el que puede describir cómo interactúa esta política con las políticas principales. Para obtener información sobre la herencia de políticas, consulte

[Descripción de la herencia de políticas de administración en la Guía](#) del AWS Organizations usuario.

Para crear una política que le permita habilitar y deshabilitar las cuentas de los miembros

1. ¿Inicia sesión con tus credenciales y abre la consola de Security Hub en la <https://console.aws.amazon.com/securityhub/v2/home? región=us-east-1>.
2. En el panel de navegación, elija Configuración y, a continuación, Configuración.
3. Elija Crear política.
4. Para obtener más información, introduzca un nombre para la política y determine si desea introducir una descripción opcional para la política.
5. Para las regiones, elija Activar todas las regiones, Desactivar todas las regiones o Especificar regiones. Si selecciona Activar todas las regiones, puede determinar si desea activar automáticamente las nuevas regiones. Si selecciona Desactivar todas las regiones, puede determinar si desea deshabilitar automáticamente las nuevas regiones. Si elige Especificar regiones, debe elegir qué regiones desea habilitar y deshabilitar.
6. (Opcional) Para obtener información sobre la configuración avanzada, consulte las [instrucciones](#) de AWS Organizations.
7. (Opcional) En el caso de las etiquetas, determine si desea añadir un par clave-valor a la política. Puede añadir hasta 50 etiquetas.
8. Elija Siguiente.
9. Revisa los cambios y, a continuación, selecciona Aplicar. Sus cuentas de destino se configuran en función de la política. Para ver la política vigente a nivel de cuenta, puede revisar la pestaña Organización de la página de configuraciones, donde puede elegir una cuenta.

Eliminar la cuenta de administrador delegado en Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Puede eliminar la cuenta de administrador delegado en la consola de Security Hub en cualquier momento. Sin embargo, esta acción no solo elimina al administrador delegado del Security Hub, sino

también al Security Hub CSPM. Recomendamos realizar esta acción únicamente cuando la haya confirmado con su cuenta de seguridad.

Note

Si utiliza una cuenta distinta de la cuenta de administración de la organización como administrador delegado de CSPM de Security Hub, si la elimina mediante la consola o la AWS Organizations API de CSPM, también se eliminará de Security Hub.

Del mismo modo, si eliminas al administrador delegado de Security Hub mediante la consola o la AWS Organizations API de Security Hub, también se eliminará del CSPM de Security Hub. Cuando el administrador delegado se retire del CSPM, Central Configuration se excluirá automáticamente.

Para eliminar la cuenta de administrador delegado

1. ¿Inicia sesión en tu AWS cuenta con las credenciales de la cuenta de administración de tu organización y abre la consola de Security Hub en la <https://console.aws.amazon.com/securityhub/versión 2/home? región=us-east-1>.
2. En el panel de navegación, elija General.
3. En Administrador delegado, elija Eliminar administrador delegado. En la ventana emergente, ingresa confirmar y selecciona Eliminar.

Recomendaciones de Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Los siguientes servicios de seguridad AWS envían los resultados a Security Hub en formato OCSF. Después de activar Security Hub, te recomendamos que los habilites Servicios de AWS para mayor seguridad.

Security Hub (CSPM)

Cuando [habilita Security Hub CSPM](#), obtiene una visión completa del estado de su seguridad. AWS Esto le ayuda a evaluar su entorno en función de los estándares y las mejores prácticas del sector

de la seguridad. Aunque puede empezar a utilizar Security Hub sin activar Security Hub CSPM, le recomendamos que active Security Hub CSPM porque Security Hub correlaciona las señales de seguridad del Security Hub CSPM para mejorar la gestión de la postura.

Si [habilitas Security Hub CSPM](#), también te recomendamos que [habilites el estándar AWS Foundational Security Best Practices](#) para tu cuenta. Este estándar consiste en un conjunto de controles que detectan cuándo usted Cuentas de AWS y sus recursos se desvían de las mejores prácticas de seguridad. Al habilitar el estándar AWS Foundational Security Best Practices para su cuenta, AWS Security Hub Cloud Security Posture Management (CSPM) habilita automáticamente todos sus controles, incluidos los controles para los siguientes tipos de recursos:

- Controles de cuenta
- Controles de DynamoDB
- EC2 Controles de Amazon
- Controles de IAM
- AWS Lambda controles
- Controles de Amazon RDS
- Controles de Amazon S3

Puede deshabilitar cualquiera de los controles de esta lista. Sin embargo, si deshabilita alguno de estos controles, no podrá recibir los resultados de exposición de los recursos compatibles. Para obtener información sobre los controles que se aplican al estándar AWS Foundational Security Best Practices v1.0.0 (FSBP), consulte el estándar [AWS Foundational Security Best Practices v1.0.0 \(FSBP\)](#).

GuardDuty

Cuando lo [habilitas GuardDuty](#), puedes ver todas las amenazas y los resultados de cobertura de seguridad en el panel de control de la consola de Security Hub. Si lo habilita GuardDuty, comienza a enviar datos GuardDuty automáticamente a Security Hub en formato OCSF.

Amazon Inspector

Al [activar Amazon Inspector](#), puede ver todas sus exposiciones y los resultados de cobertura de seguridad en el panel de control de la consola de Security Hub. Si habilitas Amazon Inspector, Amazon Inspector empezará automáticamente a enviar datos a Security Hub en formato OCSF.

Recomendamos activar el EC2 escaneo de Amazon y el escaneo estándar Lambda. Cuando activas el EC2 escaneo de Amazon, Amazon Inspector escanea EC2 las instancias de Amazon de tu cuenta para detectar vulnerabilidades en los paquetes y problemas de accesibilidad de la red. Al activar el escaneo estándar de Lambda, Amazon Inspector analiza las funciones de Lambda en busca de vulnerabilidades de software en las dependencias de los paquetes. Para obtener más información, consulte [Activación de un tipo de escaneo](#) en la Guía del usuario de Amazon Inspector.

Macie

Al [activar Macie](#), puede detectar exposiciones adicionales para sus buckets de Amazon S3. Recomendamos configurar la [detección automática de datos confidenciales](#) para que Macie pueda evaluar su inventario de cubos de Amazon S3 a diario.

Conceptos de Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Los siguientes términos y conceptos le ayudarán a entender cómo gestionar los hallazgos de exposición.

Exposición

Un posible escenario de seguridad en tu cuenta que puede deberse a vulnerabilidades, recursos explotables o errores de configuración.

Hallazgo de exposición

Tipo de hallazgo que describe una exposición presente en su entorno. Un hallazgo de exposición incluye rasgos y señales. Una señal puede incluir uno o más tipos de rasgos de exposición. Security Hub genera un hallazgo de exposición cuando las señales de Security Hub, los hallazgos de control CSPM u otros Servicios de AWS, como Amazon Inspector, indican la presencia de una exposición. Un recurso puede contener como máximo un dato de exposición. Security Hub genera un hallazgo de exposición cuando un recurso está expuesto. Si un recurso no tiene ningún rasgo de exposición o tiene rasgos insuficientes, Security Hub no genera ningún dato de exposición para ese recurso.

Señal

Un hallazgo que contribuye a un hallazgo de exposición. Una señal puede denominarse hallazgo contribuyente. Una señal puede originarse en Security Hub, CSPM u otro AWS Config Servicios de AWS, como Amazon Inspector.

Rasgo

Una desviación de seguridad que da como resultado un hallazgo de exposición. Los tipos de características incluyen la mala configuración, la accesibilidad, los datos confidenciales y la vulnerabilidad. Un rasgo está asociado a una señal y una señal puede contener varios rasgos. Por ejemplo, un control CSPM de Security Hub indica que una política gestionada por el cliente permite el control de acceso administrativo. Esta señal contiene un rasgo de configuración errónea.

Hallazgos de OCSF en Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Todos los resultados de Security Hub están formateados en el Open Cybersecurity Schema Framework (OCSF). Security Hub considera los hallazgos `activity_name != Close` como hallazgos activos. Los hallazgos activos se eliminan automáticamente si no se actualizan en 90 días. Security Hub considera los hallazgos `Activity_name = Close` como hallazgos cerrados. Los hallazgos cerrados se eliminan automáticamente si no se actualizan en 14 días. Security Hub determina cuándo se actualiza un hallazgo utilizando el valor más reciente del `hallazgomodified_time_dt`. Al final del período de retención de un hallazgo, Security Hub lo elimina permanentemente. Los proveedores de búsqueda pueden cambiar el valor del `finding.info.modified_time_dt` campo cuando actualizan un hallazgo. Para obtener información sobre otros `Activity_name` valores, consulte [Búsqueda de vulnerabilidades](#) en el esquema OCSF.

Hallazgos de cobertura en Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Los resultados de cobertura de Security Hub proporcionan visibilidad sobre qué funciones de AWS seguridad están habilitadas y dónde puede haber brechas en la cobertura en una cuenta independiente o en todo el AWS entorno de una organización. La activación de funciones de seguridad adicionales mejorará las capacidades de detección de Security Hub. Los resultados de cobertura evalúan qué GuardDuty funciones de Amazon Inspector, Macie y Security Hub CSPM están habilitadas para una cuenta. Estos hallazgos aparecen como un widget en el panel de control de Security Hub con la capacidad de obtener vistas más detalladas por capacidad de seguridad específica. Para el administrador delegado, este widget muestra un desglose de la cobertura en todas las cuentas habilitadas para Security Hub.

Limitaciones

- En el caso de las cuentas de miembros, la información de cobertura se agrega a todas las cuentas vinculadas Regiones de AWS, pero solo para esa cuenta de miembro.
- La información de cobertura no se muestra para las cuentas que no están integradas en Security Hub
- La cobertura solo indica si una Servicio de AWS está habilitada, no si están habilitadas funciones específicas de un AWS servicio.

Hallazgos de cobertura para Security Hub CSPM

Los resultados de cobertura del CSPM de Security Hub evalúan si una cuenta cuenta cuenta con un estándar de seguridad cualificado para la gestión de la postura. Se admitirá la habilitación de cualquier estándar CSPM de Security Hub, con la excepción de los estándares de AWS Control Tower etiquetado de recursos.

La detección de los estándares habilitados de forma predeterminada al habilitar Security Hub CSPM puede tardar hasta 24 horas.

Hallazgos de cobertura para GuardDuty

GuardDuty Los resultados de cobertura evalúan si GuardDuty está habilitada y qué GuardDuty funciones están habilitadas en un Cuenta de AWS:

- Protección contra malware para Amazon EC2 : analiza las EC2 instancias de Amazon en busca de malware potencial
- Amazon EKS Protection: supervisa los registros de auditoría de Kubernetes para detectar amenazas en los clústeres de Amazon EKS
- Protección Lambda: analiza las invocaciones de funciones Lambda para detectar posibles amenazas
- Protección de Amazon S3: analiza los eventos de datos para detectar posibles amenazas a los buckets de Amazon S3
- Protección de Amazon RDS: supervisa las amenazas a las bases de datos de Amazon RDS
- Supervisión del tiempo de ejecución: proporciona supervisión en tiempo real del comportamiento del tiempo de ejecución en EC2 las instancias de Amazon

Las actualizaciones de la GuardDuty cobertura pueden tardar hasta 24 horas en reflejarse en todas las cuentas de los miembros de una organización.

Hallazgos de cobertura para Amazon Inspector

Los resultados de cobertura de Amazon Inspector evalúan si Amazon Inspector está habilitado y qué funciones están habilitadas en una cuenta:

- Amazon EC2 Scanning: analiza las EC2 instancias de Amazon en busca de vulnerabilidades
- Escaneo de Amazon ECR: analiza las imágenes de los contenedores en Amazon ECR en busca de vulnerabilidades
- Escaneo estándar Lambda: analiza las funciones de Lambda en busca de vulnerabilidades
- Escaneo de código Lambda: analiza las funciones de código Lambda en busca de vulnerabilidades de código
- Amazon Inspector Code Security: analiza el código fuente de las aplicaciones propias, las dependencias de aplicaciones de terceros y la infraestructura como código en busca de vulnerabilidades

Hallazgos de cobertura para Macie

Los resultados de cobertura de Macie son evaluaciones que indican si Macie está habilitada para cruzar. Cuentas de AWS

Las actualizaciones del descubrimiento automatizado de datos confidenciales por parte de Macie pueden tardar hasta 24 horas en reflejarse en todas las cuentas de los miembros de una organización.

Hallazgos de exposición en Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Security Hub correlaciona los resultados de las comprobaciones de control del CSPM de Security Hub y otros Servicios de AWS, como Amazon Inspector, para detectar las exposiciones asociadas a los recursos. AWS Un hallazgo de exposición es un tipo de hallazgo que describe una posible exposición en su entorno debido a vulnerabilidades, recursos explotables o errores de configuración. Al priorizar y resolver las exposiciones más críticas, puede prevenir posibles ataques contra su entorno. Puede acceder a sus resultados de exposición en la consola de Security Hub y mediante programación con las operaciones de CSPM y API de Security Hub.

Tipos de recursos compatibles para los hallazgos de exposición en Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Security Hub genera resultados de exposición para los siguientes tipos AWS de recursos:

- `AWS::DynamoDB::Table`
- `AWS::EC2::Instance`
- `AWS::ECS::Service`

- `AWS::EKS::Cluster`
- `AWS::IAM::User`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::S3::Bucket`

Security Hub genera un hallazgo de exposición por recurso. Si un recurso no tiene ningún rasgo de exposición o tiene rasgos insuficientes, Security Hub no genera ningún dato de exposición para ese recurso.

Tipos de características compatibles en Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Security Hub genera un hallazgo de exposición cuando los hallazgos de control de AWS Security Hub Cloud Security Posture Management (CSPM) y los hallazgos generados por otros proveedores compatibles Servicios de AWS, como Amazon Inspector, contienen características de exposición de un recurso. La siguiente tabla proporciona información sobre los tipos de características compatibles.

Tipo de rasgo	Descripción	Origen	Recursos afectados
Configuración incorrecta	Indica un recurso mal configurado.	Hallazgos de control del CSPM de Security Hub.	Todos los tipos de recursos.
Accesibilidad	Indica las rutas de red abiertas a un recurso.	Hallazgos de control de CSPM de Security Hub y hallazgos de accesibilidad de la red	EC2 Instancias de Amazon

Tipo de rasgo	Descripción	Origen	Recursos afectados
		de Amazon Inspector.	
Información confidencial	Indica que un recurso contiene datos confidenciales.	Macie encuentra datos confidenciales.	Buckets de Amazon S3
Vulnerabilidad	Indica que un recurso está expuesto a vulnerabilidades y exposiciones comunes (CVEs).	Hallazgos de vulnerabilidad de paquetes de Amazon Inspector.	EC2 Instancias de Amazon, servicios de Amazon ECS, clústeres de Amazon EKS y funciones Lambda

Cada característica se puede asociar a varios títulos que proporcionan detalles sobre la exposición que afecta al recurso. Por ejemplo, es posible que veas un título de vulnerabilidad disponible para el rasgo de vulnerabilidad en los detalles de un hallazgo de EC2 exposición.

Generar hallazgos de exposición

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Security Hub genera datos de exposición cada 6 horas. Durante cada período de 6 horas, Security Hub considera las características de exposición disponibles para un recurso. Produce como máximo un hallazgo de exposición por ID de recurso. La exclusividad de un hallazgo viene determinada por el identificador Región de AWS, el tipo y la cuenta. Esto significa que puede tener dos recursos con el mismo ID, pero los recursos serían de tipos de recursos diferentes. Este resultado de exposición agrega todos los rasgos de exposición aplicables al recurso.

Si un recurso no tiene ningún rasgo de exposición o tiene rasgos insuficientes, Security Hub no genera ningún dato de exposición para ese recurso. Security Hub no publica las conclusiones de exposición para los tipos de recursos que no respaldan las conclusiones de exposición. Cuando un recurso tiene un número significativo y una combinación de características, Security Hub genera un hallazgo de exposición. El número y la combinación de rasgos también determinan el nivel de gravedad del hallazgo de exposición.

Ejemplo de hallazgo de exposición

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Security Hub normaliza los hallazgos de exposición en el Open Cybersecurity Schema Framework (OCSF).

Ejemplo de esquema de OCSF

En el siguiente ejemplo de esquema de OCSF, el `related_events` parámetro contiene detalles exclusivos del hallazgo de exposición, como los hallazgos contribuyentes. Los hallazgos que contribuyen son los rasgos y señales asociados a un hallazgo de exposición. Un único hallazgo contribuyente puede incluir uno o más rasgos. El `observables` parámetro identifica el recurso asociado al hallazgo contribuyente. Puede ser diferente del `resources` parámetro, que identifica el recurso asociado a la constatación de exposición.

```
{
  "activity_id": 1,
  "activity_name": "Create",
  "category_name": "Findings",
  "category_uid": 2,
  "class_name": "Detection Finding",
  "class_uid": 2004,
  "cloud": {
    "account": {
      "uid": "123456789012",
      "name": "production-application"
    },
    "cloud_partition": "aws",
    "provider": "AWS",
    "region": "us-east-1"
  }
}
```

```

    },
    "finding_info": {
      "analytic": {
        "name": "Exposure",
        "type": "Rule",
        "type_id": 1,
        "uid": "0.0.1"
      },
      "created_time_dt": "2024-11-15T21:39:26.337224100Z",
      "desc": "Publicly invocable Lambda function executed outside of VPC has
vulnerability with known exploit that can be exploited from remote network",
      "finding_info.modified_time_dt": "2024-11-15T21:39:26.337224100Z",
      "related_events_count": 3,
      "related_events": [
        {
          "tags": [
            {
              "name": "Vulnerability",
              "values": [
                "Attack Vector Network",
                "EPSS Level >= High",
                "EPSS Level >= Medium",
                "Exploit Available",
                "No Privileges Required",
                "No User Interaction Required",
                "Vulnerable"
              ]
            }
          ],
          "product": {
            "uid": "arn:aws:securityhub:us-east-1::productv2/aws/inspector"
          },
          "observables": [
            {
              "type": "Resource UID",
              "type_id": 10,
              "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
            }
          ],
          "type": "Finding",
          "title": "CVE-2023-33246 - org.apache.rocketmq:rocketmq-controller",
          "uid": "arn:aws:inspector2:us-
east-1:123456789012:finding/1234567890abcdef0"

```

```

    },
    {
      "tags": [
        {
          "name": "Reachability",
          "values": [
            "Publicly Invocable"
          ]
        }
      ],
      "product": {
        "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
      },
      "observables": [
        {
          "type": "Resource UID",
          "type_id": 10,
          "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
        }
      ],
      "type": "Finding",
      "title": "Lambda function policies should prohibit public access",
      "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
    },
    {
      "tags": [
        {
          "name": "Misconfiguration",
          "values": [
            "Deployed outside VPC"
          ]
        }
      ],
      "product": {
        "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
      },
      "observables": [
        {
          "type": "Resource UID",
          "type_id": 10,
          "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"

```

```

        }
      ],
      "type": "Finding",
      "title": "Lambda functions should be in a VPC",
      "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.3/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    }
  ],
  "title": "Publicly invocable Lambda function executed outside of VPC has
vulnerability with known exploit that can be exploited from remote network",
  "types": [
    "Exposure/Potential Impact/Resource Hijacking"
  ],
  "uid": "arn:aws:securityhub:us-
east-1:123456789012:risk:1234f781c7ae7507f01e2fb460f15ca8fe7f9c95e257698a092cb74a4ea84a42"
},
"metadata": {
  "product": {
    "name": "Security Hub Exposure Analysis",
    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub-risk",
    "vendor_name": "Amazon"
  },
  "processed_time_dt": "2024-11-15T21:39:58.819Z",
  "profiles": [
    "cloud",
    "datetime"
  ],
  "version": "1.4.0-dev"
},
"resources": [
  {
    "cloud_partition": "aws",
    "region": "us-east-1",
    "tags": [
      {
        "name": "aws:cloudformation:stack-name",
        "value": "VeepLambdaRule3"
      },
      {
        "name": "aws:cloudformation:stack-id",
        "value": "arn:aws:cloudformation:us-east-1:123456789012:stack/
VeepLambdaRule3/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
      },
      {

```

```
        "name": "aws:cloudformation:logical-id",
        "value": "lambdar3function94D10D40"
      }
    ],
    "type": "AwsLambdaFunction",
    "uid": "arn:aws:lambda:us-east-1:123456789012:application-function"
  }
],
"severity": "Critical",
"severity_id": 5,
"status": "New",
"status_id": 1,
"time": 1731706766337,
"time_dt": "2024-11-15T21:39:26.337224100Z",
"type_name": "Detection Finding: Create",
"type_uid": 200401,
"vendor_attributes": {
  "severity_id": 5,
  "severity": "Critical"
}
}
```

Determinar el nivel de gravedad de un hallazgo de exposición

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Security Hub asigna a cada exposición una gravedad predeterminada de CRITICAL, HIGHMEDIUM, o LOW. Los hallazgos de exposición con una gravedad de INFORMATIONAL no se publican. Security Hub utiliza varios factores para determinar el nivel de gravedad predeterminado de un hallazgo de exposición:

- **Conocimiento:** grado en el que la exposición no es teórica, sino que se ha hecho público o se ha hecho uso de exploits automatizados. Esto se aplica a los hallazgos de exposición para EC2 instancias y funciones Lambda.
- **Facilidad de descubrimiento:** si se dispone de herramientas automatizadas, como un escaneo de puertos o una búsqueda en Internet, para descubrir el recurso en riesgo.

- **Facilidad de explotación:** facilidad con la que un agente de amenazas puede aprovechar la exposición. Por ejemplo, si existen rutas de red abiertas o metadatos mal configurados, un agente de amenazas puede aprovechar más fácilmente la exposición.
- **Probabilidad de explotación:** probabilidad de que se aproveche la exposición en los próximos 30 días. Este factor corresponde al Sistema de puntuación de protección contra exploits (EPSS) y se aplica a los hallazgos de exposición de las EC2 instancias de Amazon y las funciones de Lambda.
- **Impacto:** el daño que se produce si se lleva a cabo el exploit. Por ejemplo, una exposición podría provocar la pérdida de responsabilidad, la pérdida de disponibilidad, la pérdida de confidencialidad por la exposición de los datos o la pérdida de integridad por la corrupción de los datos.

Revisar los resultados de la exposición

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Puedes revisar todos tus hallazgos de exposición en la consola AWS de Security Hub y con la API. La página Exposiciones de la consola de Security Hub muestra todos los hallazgos de exposición activa. Los hallazgos de exposición se enumeran por gravedad decreciente. Puedes filtrar tus hallazgos de exposición añadiendo o quitando filtros con la barra de búsqueda Añadir filtro. Puedes agrupar tus hallazgos de exposición con el menú desplegable Agrupar. También puedes filtrar tus hallazgos de exposición con el menú de filtros rápidos.

Detalles de los hallazgos de exposición

Puede ver muchos detalles de un hallazgo de exposición. En la consola de Security Hub, estos detalles se dividen en pestañas. La pestaña Descripción general proporciona una instantánea del hallazgo de exposición. La pestaña Rasgos muestra los rasgos y señales asociados a un hallazgo de exposición. La pestaña Recursos proporciona detalles sobre el recurso y las etiquetas de recursos asociadas a un hallazgo de exposición. La siguiente lista proporciona descripciones de los detalles de la búsqueda de exposiciones.

- **Título de búsqueda:** el título del hallazgo de exposición.
- **Nivel de gravedad:** el nivel de gravedad del hallazgo de exposición. Security Hub utiliza el número y la combinación de características de un recurso para determinar el nivel de gravedad de un hallazgo de exposición. El nivel de gravedad puede ser CRITICALHIGH, MEDIUM, o LOW. Security

Hub no publica los hallazgos de exposición con una gravedad de `INFORMATIONAL`. Puede actualizarlo `Severity` a través de la consola de Security Hub o mediante la operación de la [BatchUpdateFindingsV2API](#).

- Descripción: la descripción del hallazgo de exposición.
- Tipo: el nombre del tipo de hallazgo de exposición. Por ejemplo, el nombre puede parecerse a algo parecido a `Exposure/Potential Impact/Resource Hijacking`.
- Cuenta: el identificador del Cuenta de AWS lugar en el que se generó el hallazgo de exposición.
- Edad: indica cuánto tiempo ha estado activo el hallazgo de exposición.
- Hora de creación: marca temporal que indica cuándo se creó el hallazgo de exposición.
- Hora de modificación: marca de tiempo que indica cuándo se actualizó por última vez el hallazgo de exposición.
- Región: el Región de AWS lugar en el que se generó el hallazgo de exposición.
- Nombre del producto: el nombre del producto que generó el hallazgo de exposición.
- Nombre de la empresa: el nombre de la empresa que generó la constatación de exposición.
- Nombre de la actividad: el nombre de la actividad.
- Estado: el estado de este hallazgo de exposición.
- ID del hallazgo: un identificador único asociado al hallazgo de exposición.
- Posible ruta de ataque (solo en la consola): una visualización interactiva muestra cómo los posibles atacantes pueden acceder a los recursos asociados a un hallazgo de exposición y hacerse con el control de ellos. Para obtener más información, consulte [Visualización de las exposiciones en Security Hub con el gráfico de la posible ruta de ataque](#).
- Rasgos: identifica los tipos de rasgos y los títulos de los rasgos asociados con el hallazgo de exposición. En la consola de Security Hub, puede ver las características por tipo de característica o señal. Esto le ayuda a analizar las conclusiones que contribuyen a ello en el contexto de la exposición relacionada.
- Recursos: identifica el recurso asociado al hallazgo de la exposición.

Revisar los detalles de los hallazgos de exposición

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

En este tema se describe cómo revisar los detalles sobre los hallazgos de exposición en la consola de Security Hub y con la API.

Revisión de los detalles de una detección de exposición en la consola de Security Hub

Para ver los detalles de un hallazgo de exposición en la consola de Security Hub

1. ¿Inicia sesión con tus credenciales y abre la consola de Security Hub en la <https://console.aws.amazon.com/securityhub/v2/home? región=us-east-1>.
2. En el panel de navegación, elija Exposiciones.
3. Elija un hallazgo de exposición del que desee ver los detalles.

Revisar los detalles de un hallazgo de exposición con la API

Puede revisar los hallazgos de exposición con la [GetFindingsV2API](#) o con la AWS CLI. Puede filtrar los resultados con el `FindingProviderFieldsTypes` parámetro y proporcionar un valor de filtro `Exposure/EC2` si solo desea mostrar los hallazgos de exposición por EC2 ejemplo. Puede filtrar por otros campos para reducir los resultados.

Comando de ejemplo:

El siguiente es un AWS CLI ejemplo que recupera las 10 conclusiones de exposición generadas más recientemente en su cuenta. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
aws securityhub get-findings-v2 \  
    --max-results '10' \  
    --filter '{"CompositeFilters": [{"StringFilters":  
[{"FieldName":"finding_info.title","Filter":  
{"Value":"GuardDuty","Comparison":"PREFIX"}} ]}]}'
```

Corregir los hallazgos de exposición

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

En los temas de esta sección se describen los riesgos de remediación de diferentes tipos Servicios de AWS.

El Remediation campo [del formato OCSF](#) contiene dos campos: remediation y references

```
"Remediation": {  
  "Recommendation": {  
    "remediation":{"desc":"String",  
    "references":["string array"]}  
  }  
},
```

Note

La guía de remediación que se proporciona en las siguientes secciones puede requerir consultas adicionales en otros AWS recursos.

Corregir las exposiciones de las tablas de DynamoDB

AWS Security Hub puede generar resultados de exposición para las tablas de DynamoDB.

En la consola de Security Hub, la tabla de DynamoDB implicada en una búsqueda de exposición y su información de identificación aparecen en la sección Recursos de los detalles de la búsqueda. De forma programática, puede recuperar los detalles de los recursos con el [GetFindingsV2](#) funcionamiento de la API Security Hub.

Tras identificar el recurso implicado en la detección de una exposición, puede eliminarlo si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus AWS costes. Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de característica.

Un único hallazgo de exposición contiene los problemas identificados en varios temas de remediación. Por el contrario, puede abordar un hallazgo de exposición y reducir su nivel de gravedad abordando solo un tema de remediación. Su enfoque de la remediación de riesgos depende de los requisitos y las cargas de trabajo de su organización.

 Note

La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros recursos. AWS

Contenido

- [Características de mala configuración en DynamoDB](#)
 - [La recuperación de la tabla de DynamoDB está deshabilitada point-in-time](#)
 - [La tabla de DynamoDB no está cubierta por un plan de respaldo](#)
 - [La tabla de DynamoDB tiene deshabilitada la protección contra la eliminación](#)

Características de mala configuración en DynamoDB

A continuación, se describen las características de errores de configuración y los pasos de corrección de las tablas de DynamoDB.

La recuperación de la tabla de DynamoDB está deshabilitada point-in-time

Habilitar la recuperación de DynamoDB point-in-time

La recuperación de point-in-time DynamoDB proporciona copias de seguridad automatizadas y continuas de los datos de las tablas de DynamoDB. Para obtener información sobre cómo restaurar una tabla de DynamoDB a un punto en el tiempo, consulte [Restauración de una tabla de DynamoDB a un punto en el tiempo en la Guía del usuario de Amazon DynamoDB](#).

La tabla de DynamoDB no está cubierta por un plan de respaldo

AWS Backup proporciona un servicio centralizado para configurar, administrar y automatizar las copias de seguridad en todos AWS los servicios, incluido DynamoDB. Sin un plan de respaldo, su mesa carece de copias de seguridad programadas y automatizadas con períodos de retención personalizables, lo que crea importantes riesgos de seguridad. Un atacante podría dañar o eliminar los datos de la tabla de forma malintencionada. Sin las copias de seguridad adecuadas, es posible que no tenga ninguna opción de recuperación más allá de la ventana de Point-in-Time recuperación (si está habilitada), lo que podría provocar una pérdida permanente de datos. Siguiendo las prácticas recomendadas de protección de datos, recomendamos cubrir las tablas de DynamoDB con un plan de respaldo.

Creación de plan de copia de seguridad

Antes de crear un plan de respaldo, determine la frecuencia de respaldo y los períodos de retención adecuados para sus datos. Para obtener información sobre cómo crear un plan de respaldo, consulte [Asignar recursos a un plan de respaldo](#) en la Guía del usuario de Amazon DynamoDB.

La tabla de DynamoDB tiene deshabilitada la protección contra la eliminación

La protección contra la eliminación evita la eliminación accidental de las tablas de DynamoDB. Cuando la protección contra la eliminación está deshabilitada, las tablas de DynamoDB son vulnerables a la eliminación involuntaria a través de acciones de la consola, llamadas a la API, comandos de CLI o procesos automatizados. Esto puede exponer su AWS entorno a la pérdida de datos, ya que una entidad no autorizada con acceso a su AWS entorno podría eliminar las tablas de forma intencionada, lo que provocaría una interrupción del servicio y una pérdida permanente de datos. Siguiendo las prácticas recomendadas de protección de datos, recomendamos habilitar la protección de datos para las tablas de DynamoDB.

Enable deletion protection (Habilitar la protección contra la eliminación)

Si administra varias tablas, considere utilizarlas AWS CloudFormation para actualizar las propiedades de las tablas de forma masiva. Puedes modificar tus AWS CloudFormation plantillas para incluir `DeletionProtectionEnabled` propiedades y actualizar tus pilas. Tras completar la corrección, comprueba que la protección contra la eliminación esté habilitada en el menú desplegable Información adicional de la pestaña Configuración de la tabla.

Corregir las exposiciones por ejemplo EC2

AWS Security Hub puede generar resultados de exposición para las instancias de Amazon Elastic Compute Cloud (EC2).

En la consola de Security Hub, la EC2 instancia implicada en un hallazgo de exposición y su información de identificación aparecen en la sección Recursos de los detalles del hallazgo. De forma programática, puede recuperar los detalles de los recursos con el [GetFindingsV2](#) funcionamiento de la API Security Hub.

Tras identificar el recurso implicado en la detección de una exposición, puede eliminarlo si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus AWS costes. Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de característica.

Un único hallazgo de exposición contiene los problemas identificados en varios temas de remediación. Por el contrario, puede abordar un hallazgo de exposición y reducir su nivel de

gravidad abordando solo un tema de remediación. Su enfoque de la remediación de riesgos depende de los requisitos y las cargas de trabajo de su organización.

 Note

La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros recursos. AWS

Contenido

- [Características de mala configuración de las instancias EC2](#)
 - [La EC2 instancia permite el acceso al IMDS mediante la versión 1](#)
 - [El rol de IAM asociado a la EC2 instancia de Amazon tiene una política de acceso administrativo](#)
 - [El rol de IAM asociado a la EC2 instancia de Amazon tiene una política de administración de servicios](#)
 - [La EC2 instancia de Amazon tiene un grupo de seguridad o ACL de red que permite el acceso SSH o RDP.](#)
 - [La EC2 instancia de Amazon tiene un grupo de seguridad abierto](#)
 - [La EC2 instancia de Amazon tiene una dirección IP pública](#)
- [EC2 Características de accesibilidad de las instancias](#)
 - [Se puede acceder a la EC2 instancia a través de Internet](#)
 - [Se puede acceder a la EC2 instancia de Amazon desde la VPC de Amazon](#)
- [Características de vulnerabilidad de EC2 las instancias](#)
 - [EC2 la instancia tiene vulnerabilidades de software que pueden explotarse en la red con una alta probabilidad de explotación](#)
 - [La EC2 instancia de Amazon tiene vulnerabilidades de software](#)

Características de mala configuración de las instancias EC2

Estas son las características de los errores de configuración de las EC2 instancias y las medidas de corrección sugeridas.

La EC2 instancia permite el acceso al IMDS mediante la versión 1

Los metadatos de la instancia son datos sobre tu EC2 instancia de Amazon que las aplicaciones pueden usar para configurar o administrar la instancia en ejecución. El servicio de metadatos de

instancia (IMDS) es un componente de la instancia que utiliza el código de instancia para acceder de forma segura a los metadatos de la instancia. Si el IMDS no está protegido adecuadamente, puede convertirse en un posible vector de ataque, ya que proporciona acceso a credenciales temporales y otros datos de configuración confidenciales. IMDSv2 proporciona una mayor protección contra la explotación mediante la autenticación orientada a la sesión, que requiere un token de sesión para las solicitudes de metadatos y limita la duración de la sesión. Siguiendo los principios de seguridad estándar, se AWS recomienda configurar las EC2 instancias de Amazon para usarlas IMDSv2 y deshabilitarlas IMDSv1.

Pruebe la compatibilidad de las aplicaciones

Antes de IMDSv2 implementarla, prueba la instancia para asegurarte de su compatibilidad con IMDSv2. Es posible que algunas aplicaciones o scripts requieran una IMDSv1 funcionalidad básica y una configuración adicional. Para obtener más información sobre las herramientas y las rutas recomendadas para probar la compatibilidad de las aplicaciones, [consulte la versión 2 de Instance Metadata Service](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

Actualice la instancia para usarla IMDSv2

Modifique las instancias existentes para usarlas IMDSv2. Para obtener más información, consulte [Modificar las opciones de metadatos de las instancias para las instancias existentes](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

Aplicar actualizaciones a las instancias de un grupo de Auto Scaling

Si su instancia forma parte de un grupo de Auto Scaling, actualice la plantilla de lanzamiento o la configuración de lanzamiento con una nueva configuración y realice una actualización de la instancia.

El rol de IAM asociado a la EC2 instancia de Amazon tiene una política de acceso administrativo

Las políticas de acceso administrativo proporcionan a EC2 las instancias de Amazon amplios permisos Servicios de AWS y recursos. Estas políticas suelen incluir permisos que no son necesarios para la funcionalidad de las instancias. Proporcionar una identidad de IAM con una política de acceso administrativo en una EC2 instancia de Amazon (en lugar del conjunto mínimo de permisos que necesita la función asociada al perfil de la instancia) puede aumentar el alcance de un ataque si la EC2 instancia de Amazon se ve comprometida. Si una instancia se ve comprometida, los atacantes podrían utilizar estos permisos excesivos para moverse lateralmente por el entorno, acceder a los datos o manipular los recursos. Siguiendo los principios de seguridad estándar, le recomendamos

que conceda los privilegios mínimos, es decir, que solo conceda los permisos necesarios para realizar una tarea.

Revise e identifique las políticas administrativas

En el panel de control de IAM, busque el rol con su nombre. Revise la política de permisos asociada a la función de IAM. Si la política es una política AWS gestionada, busque `AdministratorAccess` o `IAMFullAccess`. De lo contrario, en el documento de política, busque las declaraciones con `"Effect": "Allow", "Action": "*" y "Resource": "*"`.

Implementación del acceso a los privilegios mínimos

Sustituya las políticas administrativas por políticas que concedan únicamente los permisos específicos necesarios para que la instancia funcione. Para obtener más información sobre las prácticas recomendadas de seguridad para las funciones de IAM, consulte [Aplicar permisos con privilegios mínimos en la sección](#) Prácticas recomendadas de seguridad de la Guía del usuario. AWS Identity and Access Management Para identificar los permisos innecesarios, puede utilizar el analizador de acceso de IAM para saber cómo modificar su política en función del historial de acceso. Para obtener más información, consulte las [conclusiones sobre el acceso externo y no utilizado](#) en la Guía del AWS Identity and Access Management usuario. Como alternativa, puede crear una nueva función de IAM para evitar que otras aplicaciones que utilicen la función existente se vean afectadas. En este escenario, cree una nueva función de IAM y, a continuación, asocie la nueva función de IAM a la instancia. Para obtener instrucciones sobre cómo reemplazar un rol de IAM por una instancia, consulta [Adjuntar un rol de IAM a una instancia](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

Consideraciones sobre la configuración segura

Si se necesitan permisos administrativos de nivel de servicio para la instancia, considere la posibilidad de implementar estos controles de seguridad adicionales para mitigar el riesgo:

- Consideraciones sobre la configuración segura
 - Autenticación multifactor (MFA): la MFA agrega una capa de seguridad adicional al requerir una forma de autenticación adicional. Esto ayuda a evitar el acceso no autorizado incluso si las credenciales están comprometidas. Para obtener más información, consulte [Requerir la autenticación multifactor \(MFA\)](#) en AWS Identity and Access Management la Guía del usuario.
 - Condiciones de IAM: la configuración de los elementos de condición le permite restringir cuándo y cómo se pueden usar los permisos administrativos en función de factores como la IP de origen

o la antigüedad del MFA. Para obtener más información, consulte [las condiciones de uso en las políticas de IAM para restringir aún más el acceso](#) en la Guía del AWS Identity and Access Management usuario.

- Límites de permisos: los límites de los permisos establecen el número máximo de permisos que puede tener un rol y proporcionan barreras a los roles con acceso administrativo. Para obtener más información, consulte [Usar los límites de permisos para delegar la administración de permisos dentro de una cuenta](#) en la Guía del AWS Identity and Access Management usuario.

Aplicar actualizaciones a las instancias de un grupo de escalado automático

Para EC2 las instancias de Amazon de un grupo de AWS autoescalado, actualiza la plantilla de lanzamiento o la configuración de lanzamiento con el nuevo perfil de instancia y realiza una actualización de la instancia. Para obtener información sobre la actualización de una plantilla de lanzamiento, consulte [Modificar una plantilla de lanzamiento \(gestionar las versiones de la plantilla de lanzamiento\)](#) en la Guía del usuario de Amazon Elastic Compute Cloud. Para obtener más información, consulte [Usar una actualización de instancias para actualizar las instancias de un grupo de Auto Scaling](#). Para obtener más información sobre el uso de funciones de IAM con grupos de Auto Scaling, consulte [Función de IAM para aplicaciones que se ejecutan en EC2 instancias de Amazon](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

El rol de IAM asociado a la EC2 instancia de Amazon tiene una política de administración de servicios

Las políticas de acceso a los servicios proporcionan a las EC2 instancias de Amazon amplios permisos para acceder a los AWS servicios y recursos. Estas políticas suelen incluir permisos que no son necesarios, por ejemplo, la funcionalidad. Proporcionar una identidad de IAM con una política de acceso administrativo en una EC2 instancia de Amazon en lugar del conjunto mínimo de permisos que necesita la función asociada al perfil de la instancia puede aumentar el alcance de un ataque si una instancia se ve comprometida. Siguiendo los principios de seguridad estándar, le recomendamos que conceda el mínimo de privilegios, lo que significa que solo conceda los permisos necesarios para realizar una tarea.

Revise e identifique las políticas administrativas

En el panel de control de IAM, busque el rol con su nombre. Revise la política de permisos asociada a la función de IAM. Si la política es una política AWS gestionada, busque AdministratorAccess o IAMFullAccess. De lo contrario, en el documento de política, busque las declaraciones con "Effect": "Allow", "Action": "*" y "Resource": "*".

Implementación del acceso a los privilegios mínimos

Sustituya las políticas de administración del servicio por aquellas que concedan solo los permisos específicos necesarios para que la instancia funcione. Para obtener más información sobre las prácticas recomendadas de seguridad para las funciones de IAM, consulte [Aplicar permisos con privilegios mínimos en la sección](#) Prácticas recomendadas de seguridad de la Guía del usuario.AWS Identity and Access Management Para identificar los permisos innecesarios, puede utilizar el analizador de acceso de IAM para saber cómo modificar su política en función del historial de acceso. Para obtener más información, consulte las [conclusiones sobre el acceso externo y no utilizado](#) en la Guía del AWS Identity and Access Management usuario. Como alternativa, puede crear una nueva función de IAM para evitar que afecte a otras aplicaciones que utilizan la función existente. En este escenario, cree una nueva función de IAM y, a continuación, asocie la nueva función de IAM a la instancia. Para obtener información sobre cómo reemplazar un rol de IAM por una instancia, consulta [Adjuntar un rol de IAM a una instancia](#) en la Guía del usuario de Amazon Elastic Compute Cloud

Consideraciones sobre la configuración segura

Si se necesitan permisos administrativos de nivel de servicio para la instancia, considere la posibilidad de implementar estos controles de seguridad adicionales para mitigar el riesgo:

Consideraciones sobre la configuración segura

Si se necesitan permisos administrativos de nivel de servicio para la instancia, considere la posibilidad de implementar estos controles de seguridad adicionales para mitigar el riesgo:

- Autenticación multifactor (MFA): la MFA agrega una capa de seguridad adicional al requerir una forma de autenticación adicional. Esto ayuda a evitar el acceso no autorizado incluso si las credenciales están comprometidas. Para obtener más información, consulte [Requerir la autenticación multifactor \(MFA\)](#) en AWS Identity and Access Management la Guía del usuario.
- Condiciones de IAM: la configuración de los elementos de condición le permite restringir cuándo y cómo se pueden usar los permisos administrativos en función de factores como la IP de origen o la antigüedad del MFA. Para obtener más información, consulte [las condiciones de uso en las políticas de IAM para restringir aún más el acceso](#) en la Guía del AWS Identity and Access Management usuario.
- Límites de permisos: los límites de los permisos establecen el número máximo de permisos que puede tener un rol y proporcionan barreras a los roles con acceso administrativo. Para obtener más información, consulte [Usar los límites de permisos para delegar la administración de permisos dentro de una cuenta](#) en la Guía del AWS Identity and Access Management usuario.

Aplicar actualizaciones a las instancias del grupo Auto Scaling

Para EC2 las instancias de Amazon de un grupo de AWS autoescalado, actualiza la plantilla de lanzamiento o la configuración de lanzamiento con el nuevo perfil de instancia y realiza una actualización de la instancia. Para obtener información sobre la actualización de una plantilla de lanzamiento, consulte [Modificar una plantilla de lanzamiento \(gestionar las versiones de la plantilla de lanzamiento\)](#) en la Guía del usuario de Amazon Elastic Compute Cloud. Para obtener más información, consulte [Usar una actualización de instancias para actualizar las instancias de un grupo de Auto Scaling](#). Para obtener más información sobre el uso de funciones de IAM con grupos de Auto Scaling, consulte [Función de IAM para aplicaciones que se ejecutan en EC2 instancias de Amazon](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

La EC2 instancia de Amazon tiene un grupo de seguridad o ACL de red que permite el acceso SSH o RDP.

Los protocolos de acceso remoto, como SSH y RDP, permiten a los usuarios conectarse a las EC2 instancias de Amazon y administraras desde ubicaciones externas. Cuando los grupos de seguridad permiten el acceso sin restricciones a estos protocolos desde Internet, aumentan la superficie de ataque de sus EC2 instancias de Amazon al permitir el acceso de Internet a su instancia. Siguiendo los principios de seguridad estándar, se AWS recomienda limitar el acceso remoto a direcciones IP o rangos específicos y confiables.

1. Modifique las reglas de los grupos de seguridad

Restringe el acceso a tus EC2 instancias de Amazon a direcciones IP de confianza específicas. Limite el acceso SSH y RDP a direcciones IP de confianza específicas o utilice la notación CIDR para especificar los rangos de IP (por ejemplo, 198.168.1.0/24). Para modificar las reglas de los grupos de seguridad, consulte [Configurar las reglas de los grupos de seguridad](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

La EC2 instancia de Amazon tiene un grupo de seguridad abierto

Los grupos de seguridad actúan como firewalls virtuales para que sus EC2 instancias de Amazon controlen el tráfico entrante y saliente. Los grupos de seguridad abiertos, que permiten el acceso sin restricciones desde cualquier dirección IP, pueden exponer sus instancias a un acceso no autorizado. Siguiendo los principios de seguridad estándar, AWS recomienda restringir el acceso de los grupos de seguridad a direcciones IP y puertos específicos.

Revise las reglas de los grupos de seguridad y evalúe la configuración actual

Evalúe qué puertos están abiertos y accesibles desde amplios rangos de IP, por ejemplo(0.0.0.0/0 or ::/0). Para obtener instrucciones sobre cómo ver los detalles de los grupos de seguridad, consulte [DescribeSecurityGroups](#)la referencia del Asistente de portabilidad para la API.NET.

Modifique las reglas de los grupos de seguridad

Modifique las reglas del grupo de seguridad para restringir el acceso a rangos o direcciones IP de confianza específicos. Al actualizar las reglas del grupo de seguridad, considere separar los requisitos de acceso para los distintos segmentos de la red creando reglas para cada rango de IP de origen requerido o restringiendo el acceso a puertos específicos. Para modificar las reglas de los grupos de seguridad, consulte [Configurar las reglas de los grupos de seguridad](#) en la Guía del EC2 usuario de Amazon.

La EC2 instancia de Amazon tiene una dirección IP pública

EC2 Las instancias de Amazon con direcciones IP públicas son accesibles públicamente desde Internet. Si bien las direcciones IP públicas a veces son necesarias para las instancias que prestan servicios a clientes externos, pueden aprovecharlas para atacar a personas no autorizadas. Siguiendo los principios de seguridad estándar, se AWS recomienda limitar la exposición pública de los recursos siempre que sea posible.

Mueva la instancia a una subred privada

Si la instancia no requiere acceso directo a Internet, plantéate moverla a una subred privada dentro de tu VPC. Esto eliminará su dirección IP pública y, al mismo tiempo, le permitirá comunicarse con otros recursos de la VPC. Para obtener más información, consulta [¿Cómo muevo mi EC2 instancia de Amazon a otra subred, zona de disponibilidad o VPC?](#) en el Centro de AWS conocimiento.

Configure las instancias para que se lancen sin direcciones IP públicas

Si la instancia se lanzó en una subred pública que no requiere direcciones IP públicas, la configuración de lanzamiento se puede modificar para evitar la asignación automática de direcciones IP públicas. Esto se puede deshabilitar a nivel de subred o al lanzar instancias individuales. Para obtener más información, consulte [Modificar los atributos de dirección IP de su subred](#) en la Guía del usuario de Amazon Virtual Private Cloud y [EC2instance Dirección IP de Amazon en la](#) Guía del usuario de Amazon Elastic Compute Cloud.

Métodos de acceso alternativos

Tenga en cuenta las siguientes opciones para los métodos de acceso alternativos:

- Utilice una puerta de enlace NAT para la conectividad saliente a Internet:

En el caso de subredes privadas que requieran acceso a Internet (por ejemplo, para descargar actualizaciones), considere la posibilidad de utilizar una puerta de enlace NAT en lugar de asignar una dirección IP pública. Una puerta de enlace NAT permite que las instancias de las subredes privadas inicien conexiones salientes a Internet y, al mismo tiempo, impide las conexiones entrantes desde Internet. Para obtener más información, consulte [las puertas de enlace NAT](#) en la Guía del usuario de Amazon Virtual Private Cloud.

- Usa Elastic Load Balancing: para las instancias que ejecutan aplicaciones web, considera usar un Elastic Load Balancer (LB). LBs se puede configurar para permitir que las instancias se ejecuten en subredes privadas, mientras que el LB se ejecuta en una subred pública y gestiona el tráfico de Internet. Para obtener más información, consulte [¿Qué es Elastic Load Balancing?](#) en la Guía del usuario del AWS ELB. Consulte las [subredes del balanceador de carga](#) en la Guía AWS prescriptiva para obtener información sobre cómo elegir una estrategia de adherencia para su LB.

EC2 Características de accesibilidad de las instancias

Estas son las características de accesibilidad de las EC2 instancias y las medidas de corrección sugeridas.

Se puede acceder a la EC2 instancia a través de Internet

Las EC2 instancias de Amazon con puertos a los que se puede acceder desde Internet a través de una puerta de enlace de Internet (incluidas las instancias detrás de los balanceadores de carga de aplicaciones o los balanceadores de carga clásicos), una conexión de emparejamiento de VPC o una puerta de enlace virtual de VPN pueden exponer la instancia a Internet. Siguiendo los principios de seguridad estándar, recomendamos implementar controles de acceso a la red con privilegios mínimos restringiendo el tráfico entrante solo a las fuentes y puertos necesarios.

Modifique o elimine las reglas de los grupos de seguridad

En la pestaña Recursos, abra el recurso para Amazon EC2 Security Group. Compruebe si se requiere acceso a Internet para que la instancia funcione. Modifique o elimine las reglas de los grupos de seguridad entrantes que permiten el acceso sin restricciones (`0.0.0.0/0o::/0`). Implemente reglas más restrictivas basadas en rangos de IP o grupos de seguridad específicos. Si es necesario un acceso público limitado, restrinja el acceso a los puertos y protocolos específicos necesarios para el funcionamiento de la instancia. Para obtener instrucciones sobre la administración

de las reglas de los grupos de [seguridad, consulte Configurar las reglas de los grupos](#) de seguridad en la Guía del EC2 usuario de Amazon.

Actualice la red ACLs

Revise y modifique las listas de control de acceso a la red (ACLs) asociadas a la subred de la instancia. Compruebe que la configuración de la ACL se ajuste a los cambios del grupo de seguridad y no permita el acceso público de forma involuntaria. Para obtener instrucciones sobre cómo modificar la red ACLs, consulte [Trabajar con la red ACLs](#) en la Guía del usuario de Amazon VPC.

Métodos de acceso alternativos

Tenga en cuenta las siguientes opciones para los métodos de acceso alternativos:

- Utilice la puerta de enlace NAT para la conectividad saliente a Internet: en los casos de subredes privadas que requieren acceso a Internet (por ejemplo, para descargar actualizaciones), considere la posibilidad de utilizar una puerta de enlace NAT en lugar de asignar una dirección IP pública. Una puerta de enlace NAT permite que las instancias de subredes privadas inicien conexiones salientes a Internet y, al mismo tiempo, impide las conexiones entrantes desde Internet.
- Utilice el administrador de sesiones de Systems Manager: el administrador de sesiones proporciona un acceso seguro desde el shell a sus EC2 instancias de Amazon sin necesidad de puertos de entrada, administrar claves SSH ni mantener hosts bastiones.
- Utilice WAF y Elastic Load Balancing o Application Load Balancer: en el caso de las instancias que ejecutan aplicaciones web, considere la posibilidad de utilizar un LB combinado AWS con Web Application Firewall (WAF). LBs se puede configurar para permitir que las instancias se ejecuten en subredes privadas mientras que el LB se ejecuta en una subred pública y gestiona el tráfico de Internet. Añadir un WAF a tu balanceador de cargas proporciona protección adicional contra los exploits web y los bots.

Se puede acceder a la EC2 instancia de Amazon desde la VPC de Amazon

Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar AWS recursos en una red virtual definida. Las configuraciones de red de Amazon VPC que permiten el acceso sin restricciones entre instancias pueden aumentar el alcance de un ataque si una instancia se ve comprometida. Siguiendo las mejores prácticas de seguridad, AWS recomienda implementar la segmentación de la red y los controles de acceso con privilegios mínimos a nivel de subred y grupo de seguridad.

Revise los patrones de conectividad de red de Amazon VPC

En el hallazgo de exposición, identifique el ID del grupo de seguridad en el ARN. Identifique qué instancias deben comunicarse entre sí y en qué puertos. Puede usar Amazon VPC Flow Logs para analizar los patrones de tráfico existentes en su Amazon VPC y así identificar qué puertos se están utilizando.

Modifique las reglas de los grupos de seguridad

Modifique las reglas del grupo de seguridad para restringir el acceso a rangos o direcciones IP de confianza específicos. Por ejemplo, en lugar de permitir todo el tráfico de todo el rango CIDR de la VPC (por ejemplo, 10.0.0.0/16), restrinja el acceso a grupos de seguridad o rangos de IP específicos. Al actualizar las reglas de los grupos de seguridad, considere la posibilidad de separar los requisitos de acceso para los diferentes segmentos de la red mediante la creación de reglas para cada rango de IP de origen requerido o la restricción del acceso a puertos específicos. Para modificar las reglas de los grupos de seguridad, consulte [Configurar las reglas de los grupos de seguridad](#) en la Guía del EC2 usuario de Amazon.

Considere la posibilidad de organizar los recursos de Amazon VPC en subredes en función de las funciones o los requisitos de seguridad. Por ejemplo, coloque los servidores web y los servidores de bases de datos en subredes independientes. Para obtener más información, consulte [Subredes para su VPC](#) en la Guía del usuario de Amazon Virtual Private Cloud.

Configure la red ACLs para la protección a nivel de subred

Las listas de control de acceso a la red (NACLs) proporcionan un nivel de seguridad adicional a nivel de subred. A diferencia de los grupos de seguridad, no NACLs tienen estado y requieren que las reglas de entrada y salida estén definidas de forma explícita. Para obtener más información, consulte [Control del tráfico de subred con listas de control de acceso a la red](#) en la Guía del usuario de Amazon Virtual Private Cloud.

Consideraciones adicionales

Tenga en cuenta lo siguiente a la hora de restringir el acceso a su Amazon VPC

- Emparejamiento de Amazon VPC o Transit Gateway con enrutamiento restrictivo: si su arquitectura utiliza varios dispositivos VPCs que necesitan comunicarse, considere la posibilidad de utilizar AWS Transit Gateway y Amazon VPC peering para proporcionar conectividad entre Amazon y, al VPCs mismo tiempo, controlar qué subredes se pueden comunicar entre sí. [Para obtener más información, consulte Cómo empezar a usar Amazon VPC Transit Gateways y las conexiones de peering de VPC.](#)

- Puntos de enlace de servicio y enlaces privados: los puntos de enlace de Amazon VPC se pueden utilizar para mantener el tráfico dentro de AWS la red y comunicarse AWS con los recursos en lugar de hacerlo a través de Internet. Esto reduce la necesidad de conectividad directa entre las instancias que acceden a los mismos servicios. Para obtener información sobre los puntos de enlace de VPC, consulte [¿Qué son los puntos de enlace de Amazon VPC?](#) en la Guía del usuario de Amazon Virtual Private Cloud. Para la conectividad con los servicios alojados en otros Amazon VPCs, considere utilizar AWS PrivateLink.

Características de vulnerabilidad de EC2 las instancias

Estos son los rasgos de vulnerabilidad de las EC2 instancias y las medidas de corrección sugeridas.

EC2 la instancia tiene vulnerabilidades de software que pueden explotarse en la red con una alta probabilidad de explotación

Los paquetes de software que se instalan en EC2 las instancias pueden estar expuestos a vulnerabilidades y exposiciones comunes (). CVEs Las críticas CVEs representan riesgos de seguridad importantes para su AWS entorno. Los responsables no autorizados pueden aprovechar estas vulnerabilidades no corregidas para comprometer la confidencialidad, la integridad o la disponibilidad de los datos, o para acceder a otros sistemas. Las vulnerabilidades críticas con una alta probabilidad de explotación representan amenazas inmediatas para la seguridad, ya que es posible que los atacantes o las herramientas de escaneo automatizadas ya estén disponibles públicamente y que los atacantes o las herramientas de escaneo automatizadas lo utilicen activamente. Recomendamos parchear estas vulnerabilidades para proteger la instancia.

Actualice las instancias afectadas

Consulta la sección Referencias de la pestaña Vulnerabilidad de la característica. La documentación del proveedor puede incluir una guía de remediación específica. Siga las medidas correctivas adecuadas siguiendo estas pautas generales:

Utilice el Administrador de parches de Systems Manager para aplicar parches tanto a los sistemas operativos como a las aplicaciones. Patch Manager le ayuda a seleccionar e implementar automáticamente los parches del sistema operativo y del software en grandes grupos de instancias. Si no tiene configurado el Administrador de parches, actualice manualmente el sistema operativo en cada instancia afectada.

Actualice las aplicaciones afectadas a sus últimas versiones seguras siguiendo los procedimientos recomendados por el proveedor. Para gestionar las actualizaciones de las aplicaciones en varias

instancias, considere la posibilidad de utilizar Systems Manager State Manager para mantener el software en un estado uniforme. Si no hay actualizaciones disponibles, considere la posibilidad de eliminar o deshabilitar la aplicación vulnerable hasta que se publique un parche u otras medidas de mitigación, como restringir el acceso de red a la aplicación o deshabilitar las funciones vulnerables.

Siga los consejos de remediación específicos que se proporcionan en el hallazgo de Amazon Inspector. Esto podría implicar cambiar las reglas de los grupos de seguridad, modificar las configuraciones de las instancias o ajustar la configuración de la aplicación.

Compruebe si la instancia forma parte de Auto Scaling Group. Los parches de reemplazo de la AMI se realizan en infraestructuras inmutables mediante la actualización del ID de AMI que está configurado para implementar nuevas instancias de Amazon en EC2 un grupo de Auto Scaling. Si utiliza una custom/golden AMI, cree una instancia con la nueva AMI y, a continuación, personalice la instancia y cree una nueva AMI dorada. Para obtener más información, consulte la [AMI actualiza la aplicación de parches \(uso de parches AMIs para grupos de Auto Scaling\)](#).

Consideraciones futuras

Para evitar que ocurran en el futuro, considere la posibilidad de implementar un programa de administración de vulnerabilidades. Amazon Inspector se puede configurar para CVEs que escanee automáticamente sus instancias. Amazon Inspector también se puede integrar con Security Hub para realizar correcciones automáticas. Considere la posibilidad de implementar un programa de parches regular mediante Windows de mantenimiento de Systems Manager para minimizar las interrupciones en sus instancias.

La EC2 instancia de Amazon tiene vulnerabilidades de software

Los paquetes de software que están instalados en Amazon EC2 instancias pueden estar expuestos a vulnerabilidades y exposiciones comunes (CVEs). Los no críticos CVEs representan debilidades de seguridad con menor gravedad o capacidad de explotación en comparación con los críticos. CVEs Si bien estas vulnerabilidades representan un riesgo menos inmediato, los atacantes aún pueden aprovechar estas vulnerabilidades sin parches para comprometer la confidencialidad, la integridad o la disponibilidad de los datos, o para acceder a otros sistemas. Siguiendo las prácticas recomendadas de seguridad, AWS recomienda parchar estas vulnerabilidades para proteger la instancia de los ataques.

Actualiza las instancias afectadas

Utilice el Administrador de parches de AWS Systems Manager para aplicar parches a los sistemas operativos. Patch Manager le ayuda a seleccionar e implementar automáticamente los parches

del sistema operativo y del software en grandes grupos de instancias. Si no tiene configurado el Administrador de parches, actualice manualmente el sistema operativo en cada instancia afectada.

Actualice las aplicaciones afectadas a sus últimas versiones seguras siguiendo los procedimientos recomendados por el proveedor. Para gestionar las actualizaciones de las aplicaciones en varias instancias, considere la posibilidad de utilizar AWS Systems Manager State Manager para mantener el software en un estado uniforme. Si no hay actualizaciones disponibles, considere la posibilidad de eliminar o deshabilitar la aplicación vulnerable hasta que se publique un parche u otras medidas de mitigación, como restringir el acceso de red a la aplicación o deshabilitar las funciones vulnerables.

Siga los consejos de remediación específicos que se proporcionan en el hallazgo de Amazon Inspector. Esto podría implicar cambiar las reglas de los grupos de seguridad, modificar las configuraciones de las instancias o ajustar la configuración de la aplicación.

Compruebe si la instancia forma parte de Auto Scaling Group. Los parches de reemplazo de la AMI se realizan en infraestructuras inmutables mediante la actualización del ID de AMI que está configurado para implementar nuevas instancias de Amazon en EC2 un grupo de Auto Scaling. Si utiliza una custom/golden AMI, cree una instancia con la nueva AMI y, a continuación, personalice la instancia y cree una nueva AMI dorada. Para obtener más información, consulte la [AMI actualiza la aplicación de parches \(uso de parches AMIs para grupos de Auto Scaling\)](#).

Consideraciones futuras

Para evitar que ocurran en el futuro, considere la posibilidad de implementar un programa de administración de vulnerabilidades. Amazon Inspector se puede configurar para CVEs que escanee automáticamente sus instancias. Amazon Inspector también se puede integrar con Security Hub para realizar correcciones automáticas. Considere la posibilidad de implementar un programa de parches regular mediante Windows de mantenimiento de Systems Manager para minimizar las interrupciones en sus instancias.

Corregir las exposiciones de los servicios de Amazon ECS

AWS Security Hub puede generar datos de exposición para los servicios de Amazon Elastic Container Service (Amazon ECS).

El servicio Amazon ECS implicado en la detección de una exposición y su información de identificación figuran en la sección Recursos de los detalles de la búsqueda. Puede recuperar estos detalles de los recursos en la consola de Security Hub o mediante programación mediante el [GetFindingsV2](#) funcionamiento de la API de Security Hub.

Tras identificar el recurso implicado en la detección de una exposición, puede eliminarlo si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus AWS costes. Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de característica.

Un único hallazgo de exposición contiene los problemas identificados en varios temas de remediación. Por el contrario, puede abordar un hallazgo de exposición y reducir su nivel de gravedad abordando solo un tema de remediación. Su enfoque de la remediación de riesgos depende de los requisitos y las cargas de trabajo de su organización.

Note

La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros recursos. AWS

Contenido

- [Características de mala configuración de los servicios de Amazon ECS](#)
 - [El servicio Amazon ECS utiliza una definición de tareas configurada con privilegios elevados.](#)
 - [El servicio Amazon ECS tiene un contenedor que puede asumir una función de IAM](#)
 - [El servicio Amazon ECS utiliza una definición de tareas que permite a los contenedores acceder a los sistemas de archivos raíz.](#)
 - [El servicio Amazon ECS utiliza una definición de tarea configurada para compartir el espacio de nombres de procesos de un host.](#)
 - [El servicio Amazon ECS utiliza una definición de tarea configurada con credenciales de texto sin cifrar en las variables de entorno.](#)
 - [El servicio Amazon ECS tiene un grupo de seguridad abierto](#)
 - [El servicio Amazon ECS tiene una dirección IP pública](#)
 - [El servicio Amazon ECS utiliza una definición de tareas que se configura con el modo de red de host activado.](#)
 - [La función de IAM asociada al servicio Amazon ECS tiene una política de acceso administrativo.](#)
- [Características de vulnerabilidad de los servicios de Amazon ECS](#)
 - [El servicio Amazon ECS tiene un contenedor con vulnerabilidades de software que pueden explotarse en la red con una alta probabilidad de explotación](#)
 - [El servicio Amazon ECS tiene un contenedor con vulnerabilidades de software](#)

Características de mala configuración de los servicios de Amazon ECS

A continuación, se indican las características de los errores de configuración de los servicios de Amazon ECS y se sugieren los pasos para corregirlos.

El servicio Amazon ECS utiliza una definición de tareas configurada con privilegios elevados.

Los contenedores de Amazon ECS que se ejecutan con privilegios elevados tienen capacidades similares a las del sistema anfitrión, lo que podría permitir el acceso a los recursos del host y a otros contenedores. Esta configuración aumenta el riesgo de que un contenedor comprometido se utilice para acceder a recursos o modificarlos fuera del alcance previsto, lo que podría provocar la fuga del contenedor, el acceso no autorizado al host subyacente y las infracciones que afecten a otros contenedores del mismo host. Siguiendo los principios de seguridad estándar, se AWS recomienda conceder los privilegios mínimos, es decir, conceder únicamente los permisos necesarios para realizar una tarea.

Revise y modifique la definición de la tarea

En la exposición, identifique el ARN de la definición de la tarea. Abra la definición de la tarea en la consola de Amazon ECS. En la definición de la tarea, busque el indicador de privilegio establecido en true en las definiciones del contenedor. Si no se requiere el modo privilegiado, cree una nueva revisión de la definición de tareas sin el indicador privilegiado. Si se requiere el modo privilegiado, considere la posibilidad de configurar el contenedor para que utilice un sistema de archivos de solo lectura a fin de evitar modificaciones no autorizadas.

El servicio Amazon ECS tiene un contenedor que puede asumir una función de IAM

Los roles de IAM permiten que las tareas de Amazon ECS accedan de forma segura a otros AWS servicios mediante credenciales temporales. Es posible que se requieran funciones de ejecución de tareas para las tareas de Amazon ECS en las que el contenedor deba interactuar con otros AWS recursos. Si bien esto a veces es necesario para el funcionamiento del contenedor, las funciones mal configuradas pueden otorgar privilegios excesivos que los atacantes pueden aprovechar si un contenedor se ve comprometido, lo que podría permitir el acceso no autorizado a AWS los recursos, el robo de datos o la modificación no autorizada de la infraestructura. Siguiendo los principios de seguridad estándar, AWS recomienda implementar el acceso con privilegios mínimos y revisar las funciones de IAM asociadas a sus tareas de Amazon ECS.

Revise las funciones adjuntas

Ve al panel de control de IAM y selecciona el rol identificado. Revise la política de permisos asociada a la función de IAM. Si la tarea requiere la interacción con otros AWS servicios, mantenga la función

de ejecución de la tarea y considere la posibilidad de aplicar permisos con privilegios mínimos. De lo contrario, cree una nueva revisión de la definición de la tarea sin la función de ejecución.

El servicio Amazon ECS utiliza una definición de tareas que permite a los contenedores acceder a los sistemas de archivos raíz.

Los contenedores de Amazon ECS con acceso al sistema de archivos raíz del host pueden leer, modificar o ejecutar archivos críticos en el sistema host. Esta configuración aumenta el riesgo de que un contenedor comprometido se utilice para acceder a recursos o modificarlos fuera del alcance previsto, lo que podría exponer datos confidenciales del sistema de archivos anfitrión. Siguiendo los principios de seguridad estándar, se AWS recomienda conceder el mínimo de privilegios, lo que significa que se concedan únicamente los permisos necesarios para realizar una tarea.

Revise y modifique los contenedores con acceso al sistema de archivos del host

En el hallazgo de exposición, identifique el ARN de la definición de la tarea. Abra la definición de la tarea en la consola de Amazon ECS. Busque la sección de volúmenes en la definición de la tarea que define las asignaciones de rutas de los hosts. Revise la definición de la tarea para determinar si es necesario acceder al sistema de archivos del host para que funcione el contenedor. Si no es necesario acceder al sistema de archivos del host, cree una nueva revisión de la definición de la tarea y elimine cualquier definición de volumen que utilice las rutas del host. Si es necesario acceder al sistema de archivos del host, considere la posibilidad de configurar el contenedor para que utilice un sistema de archivos de solo lectura a fin de evitar modificaciones no autorizadas.

El servicio Amazon ECS utiliza una definición de tarea configurada para compartir el espacio de nombres de procesos de un host.

Los contenedores de Amazon ECS que se ejecutan con espacios de nombres expuestos pueden acceder a los recursos del sistema anfitrión y a otros espacios de nombres de contenedores. Esta configuración podría permitir que un contenedor comprometido escape de su límite de aislamiento, lo que podría provocar el acceso a procesos, interfaces de red u otros recursos fuera del alcance previsto. Un espacio de nombres de ID de proceso (PID) proporciona separación entre los procesos. Evita que los procesos del sistema sean visibles y PIDs permite su reutilización, incluido el PID 1. Si el espacio de nombres PID del host se comparte con los contenedores, los contenedores podrían ver todos los procesos del sistema anfitrión. Esto reduce la ventaja del aislamiento a nivel de proceso entre el host y los contenedores. Estos factores podrían provocar el acceso no autorizado a los procesos del propio servidor, incluida la posibilidad de manipularlos y cancelarlos. Siguiendo los principios de seguridad estándar, AWS recomienda mantener un aislamiento adecuado del espacio de nombres para los contenedores.

Actualice las definiciones de las tareas con los espacios de nombres expuestos

Abra la pestaña Recursos de la exposición e identifique la definición de la tarea con el espacio de nombres expuesto. Abra la definición de la tarea en la consola de Amazon ECS. Busque la configuración de PIDMode con el valor host, lo que compartiría los espacios de nombres de los ID del proceso con el host. Elimine la configuración PIDMode: host de las definiciones de tareas para garantizar que los contenedores se ejecuten con el aislamiento adecuado del espacio de nombres.

El servicio Amazon ECS utiliza una definición de tarea configurada con credenciales de texto sin cifrar en las variables de entorno.

Los contenedores de Amazon ECS con credenciales de texto sin cifrar en las variables de entorno exponen información de autenticación confidencial que podría verse comprometida si un atacante obtiene acceso a la definición de la tarea, al entorno del contenedor o a los registros del contenedor. Esto supone un riesgo de seguridad importante, ya que las credenciales filtradas podrían utilizarse para acceder a otros AWS servicios o recursos.

Sustituya las credenciales de texto no cifrado

En la búsqueda de exposición, identifique la definición de la tarea con credenciales de texto sin cifrar. Abra la definición de la tarea en la consola de Amazon ECS. Busque variables de entorno en la definición del contenedor que contengan valores confidenciales, como claves de AWS acceso, contraseñas de bases de datos o tokens de API.

Considere las siguientes alternativas para transferir credenciales:

- En lugar de utilizar claves de AWS acceso, utilice funciones de ejecución de tareas y funciones de tareas de IAM para conceder permisos a sus contenedores.
- Guarde las credenciales como secretas en AWS Secrets Manager y haga referencia a ellas en la definición de la tarea.

Actualizar definiciones de tareas

Cree una nueva revisión de la definición de la tarea que gestione las credenciales de forma segura. A continuación, actualice su servicio Amazon ECS para utilizar la nueva revisión de la definición de tareas.

El servicio Amazon ECS tiene un grupo de seguridad abierto

Los grupos de seguridad actúan como firewalls virtuales para sus tareas de Amazon ECS a fin de controlar el tráfico entrante y saliente. Los grupos de seguridad abiertos, que permiten el acceso sin restricciones desde cualquier dirección IP, pueden exponer sus contenedores a un acceso no autorizado, lo que aumenta el riesgo de exposición a herramientas de escaneo automatizadas y a ataques dirigidos. Siguiendo los principios de seguridad estándar, AWS recomienda restringir el acceso de los grupos de seguridad a direcciones IP y puertos específicos.

Revise las reglas de los grupos de seguridad y evalúe la configuración actual

Abra el recurso del grupo de seguridad Amazon ECS. Evalúe qué puertos están abiertos y accesibles desde amplios rangos de IP, por ejemplo(`0.0.0.0/0` or `::/0`).

Modifique las reglas de los grupos de seguridad

Modifique las reglas del grupo de seguridad para restringir el acceso a rangos o direcciones IP de confianza específicos. Al actualizar las reglas del grupo de seguridad, considere separar los requisitos de acceso para los distintos segmentos de la red creando reglas para cada rango de IP de origen requerido o restringiendo el acceso a puertos específicos.

Modifique las reglas de los grupos de seguridad

Tenga en cuenta las siguientes opciones para los métodos de acceso alternativos:

- Session Manager proporciona un acceso seguro desde el shell a sus EC2 instancias de Amazon sin necesidad de puertos de entrada, administrar claves SSH ni mantener hosts bastiones.
- NACLs proporcionan una capa adicional de seguridad a nivel de subred. A diferencia de los grupos de seguridad, no NACLs tienen estado y requieren que las reglas de entrada y salida se definan de forma explícita.

El servicio Amazon ECS tiene una dirección IP pública

Se puede acceder directamente a los servicios de Amazon ECS con direcciones IP públicas asignadas a sus tareas desde Internet. Si bien esto puede ser necesario para los servicios que deben estar disponibles públicamente, aumenta la superficie de ataque y la posibilidad de acceso no autorizado.

Identifique los servicios con direcciones IP públicas

En el hallazgo de exposición, identifique el servicio Amazon ECS que tiene direcciones IP públicas asignadas a sus tareas. Busque la `assignPublicIp` configuración con un valor de `ENABLED` en la configuración del servicio.

Actualizar definiciones de tareas

Cree una nueva revisión de la definición de la tarea que deshabilite las direcciones IP públicas. A continuación, actualice su servicio Amazon ECS para utilizar la nueva revisión de la definición de tareas.

Implemente patrones de acceso a redes privadas

Para las instancias que ejecutan aplicaciones web, considere la posibilidad de utilizar un Load Balancer (LB). LBs se puede configurar para permitir que las instancias se ejecuten en subredes privadas mientras que el LB se ejecuta en una subred pública y gestiona el tráfico de Internet.

El servicio Amazon ECS utiliza una definición de tareas que se configura con el modo de red de host activado.

Los contenedores de Amazon ECS que se ejecutan en el modo de red de host comparten el espacio de nombres de la red con el host, lo que permite el acceso directo a las interfaces de red, los puertos y las tablas de enrutamiento del host. Esta configuración evita el aislamiento de red que proporcionan los contenedores, lo que podría exponer los servicios que se ejecutan en el contenedor directamente a redes externas y permitir que los contenedores modifiquen la configuración de la red del host. Siguiendo los principios de seguridad estándar, AWS recomienda mantener un aislamiento de red adecuado para los contenedores.

Deshabilite el modo de red del host

En el hallazgo de exposición, identifique la definición de la tarea con el modo de red host. Abra la definición de la tarea en la consola de Amazon ECS. Busque la configuración `NetworkMode` con el valor `host` en la definición de la tarea.

Tenga en cuenta las siguientes opciones para deshabilitar el modo de red del host:

- El modo `awsvpc` de red proporciona el mayor nivel de aislamiento de la red, ya que proporciona a cada tarea su propia interface de red elástica.
- El modo `bridge` de red proporciona aislamiento y, al mismo tiempo, permite que las asignaciones de puertos expongan puertos contenedores específicos al host.

Actualizar definiciones de tareas

Cree una nueva revisión de la definición de la tarea con la configuración del modo de red actualizada. A continuación, actualice su servicio Amazon ECS para utilizar la nueva revisión de la definición de tareas.

La función de IAM asociada al servicio Amazon ECS tiene una política de acceso administrativo.

Las funciones de IAM con políticas de acceso administrativo adjuntas a las tareas de Amazon ECS proporcionan amplios permisos que superan lo que normalmente se requiere para el funcionamiento de los contenedores. Esta configuración aumenta el riesgo de que un contenedor comprometido se utilice para acceder a los recursos de su AWS entorno o modificarlos. Siguiendo los principios de seguridad estándar, AWS recomienda implementar el acceso con privilegios mínimos concediendo solo los permisos necesarios para que una tarea funcione.

Revise e identifique las políticas administrativas

En el ID del recurso, identifique el nombre del rol de IAM. Vaya al panel de control de IAM y seleccione el rol identificado. Revise la política de permisos asociada a la función de IAM. Si la política es una política AWS gestionada, busque `AdministratorAccess`. De lo contrario, en el documento de política, busque las declaraciones que contengan las declaraciones `"Effect": "Allow"`, `"Action": "*"` , and `"Resource": "*"` juntas.

Implementación del acceso a los privilegios mínimos

Sustituya las políticas administrativas por aquellas que concedan únicamente los permisos específicos necesarios para que la instancia funcione. Para identificar los permisos innecesarios, puede utilizar el analizador de acceso de IAM para saber cómo modificar su política en función del historial de acceso. Como alternativa, puede crear una nueva función de IAM para evitar que afecte a otras aplicaciones que utilizan la función existente. En este escenario, cree una nueva función de IAM y, a continuación, asocie la nueva función de IAM a la instancia.

Consideraciones sobre la configuración segura

Si se necesitan permisos administrativos de nivel de servicio para la instancia, considere la posibilidad de implementar estos controles de seguridad adicionales para mitigar el riesgo:

- La MFA añade una capa de seguridad adicional al requerir una forma adicional de autenticación. Esto ayuda a evitar el acceso no autorizado incluso si las credenciales están comprometidas.

- La configuración de los elementos de condición le permite restringir cuándo y cómo se pueden usar los permisos administrativos en función de factores como la IP de origen o la antigüedad del MFA.

Actualizar definiciones de tareas

Cree una nueva revisión de la definición de la tarea que haga referencia a las funciones de IAM nuevas o actualizadas. A continuación, actualice su servicio Amazon ECS para utilizar la nueva revisión de la definición de tareas.

Características de vulnerabilidad de los servicios de Amazon ECS

Estas son las características de accesibilidad de Amazon ECS y las medidas de corrección sugeridas.

El servicio Amazon ECS tiene un contenedor con vulnerabilidades de software que pueden explotarse en la red con una alta probabilidad de explotación

1. Comprenda la exposición

Los hallazgos de vulnerabilidades de los paquetes identifican los paquetes de software de su AWS entorno que están expuestos a vulnerabilidades y exposiciones comunes (CVEs). Los atacantes pueden aprovechar las vulnerabilidades no parcheadas y poner en riesgo la confidencialidad, integridad o disponibilidad de los datos, así como acceder a otros sistemas. Las imágenes de los contenedores ECR pueden contener hallazgos de vulnerabilidades en los paquetes.

2. Remedie la exposición

a. Actualice la versión del paquete

Revise el hallazgo de vulnerabilidad del paquete para su función Lambda. Actualice la versión del paquete según lo sugerido por Amazon Inspector. Para obtener más información, consulta [Cómo ver los detalles de las conclusiones de Amazon Inspector](#) en la Guía del usuario de Amazon Inspector. La sección Remediación de los detalles de búsqueda de la consola de Amazon Inspector le indica qué comandos puede ejecutar para actualizar el paquete.

b. Actualice las imágenes del contenedor base

Reconstruye y actualiza las imágenes del contenedor base con regularidad para mantenerlos actualizados. Al reconstruir la imagen, no incluya componentes innecesarios para reducir la superficie de ataque. Para obtener instrucciones sobre cómo reconstruir una imagen de contenedor, consulte [Reconstruir imágenes con frecuencia](#).

El servicio Amazon ECS tiene un contenedor con vulnerabilidades de software

Los paquetes de software que se instalan en los contenedores de Amazon ECS pueden estar expuestos a vulnerabilidades y exposiciones comunes (CVEs). Las vulnerabilidades de baja prioridad representan debilidades de seguridad con menor gravedad o capacidad de explotación en comparación con las vulnerabilidades de alta prioridad. Si bien estas vulnerabilidades representan un riesgo menos inmediato, los atacantes pueden aprovechar estas vulnerabilidades sin parches para comprometer la confidencialidad, la integridad o la disponibilidad de los datos, o para acceder a otros sistemas.

Actualice las imágenes de los contenedores afectados

Consulta la sección Referencias de la pestaña Vulnerabilidad de la característica. La documentación del proveedor puede incluir una guía de remediación específica.

Aplique las medidas correctivas adecuadas siguiendo estas pautas generales:

- Actualice las imágenes del contenedor para usar versiones parcheadas de los paquetes afectados.
- Actualiza las dependencias afectadas de tu aplicación a sus últimas versiones seguras.

Tras actualizar la imagen del contenedor, envíala al registro del contenedor y actualiza la definición de tareas de Amazon ECS para usar la nueva imagen.

Consideraciones futuras

Para reforzar aún más la postura de seguridad de las imágenes de sus contenedores, considere seguir las prácticas recomendadas de seguridad de contenedores y tareas de Amazon ECS. Amazon Inspector se puede configurar para CVEs que escanee automáticamente sus contenedores. Amazon Inspector también se puede integrar con Security Hub para realizar correcciones automáticas. Considere la posibilidad de implementar un programa de parches regular mediante Windows de mantenimiento de Systems Manager para minimizar las interrupciones en sus contenedores.

Corregir las exposiciones de los clústeres de Amazon EKS

AWS Security Hub puede generar resultados de exposición para los clústeres de Amazon Elastic Kubernetes Service (Amazon EKS).

El clúster Amazon EKS implicado en un hallazgo de exposición y su información de identificación figuran en la sección Recursos de los detalles del hallazgo. Puede recuperar estos detalles

de los recursos en la consola de Security Hub o mediante programación mediante el [GetFindingsV2](#) funcionamiento de la API de Security Hub.

Tras identificar el recurso implicado en la detección de una exposición, puede eliminarlo si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus AWS costes. Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de característica.

Un único hallazgo de exposición contiene los problemas identificados en varios temas de remediación. Por el contrario, puede abordar un hallazgo de exposición y reducir su nivel de gravedad abordando solo un tema de remediación. Su enfoque de la remediación de riesgos depende de los requisitos y las cargas de trabajo de su organización.

 Note

La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros recursos. AWS

Contenido

- [Características de mala configuración de los clústeres de Amazon EKS](#)
 - [El clúster Amazon EKS permite el acceso público](#)
 - [El clúster de Amazon EKS utiliza una versión de Kubernetes no compatible](#)
 - [El clúster de Amazon EKS utiliza secretos de Kubernetes no cifrados](#)
- [Características de vulnerabilidad de los clústeres de Amazon KES](#)
 - [El clúster Amazon EKS tiene un contenedor con vulnerabilidades de software explotables en red con una alta probabilidad de explotación](#)
 - [El clúster Amazon EKS tiene un contenedor con vulnerabilidades de software](#)

Características de mala configuración de los clústeres de Amazon EKS

A continuación, se muestran las características de configuración errónea de los clústeres de Amazon EKS y se sugieren los pasos de corrección.

El clúster Amazon EKS permite el acceso público

El punto de enlace del clúster Amazon EKS es el punto de enlace que se utiliza para comunicarse con el servidor de API de Kubernetes del clúster. De forma predeterminada, este punto final es

público en Internet. Los puntos finales públicos aumentan la superficie de ataque y el riesgo de acceso no autorizado al servidor API de Kubernetes, lo que podría permitir a los atacantes acceder a los recursos del clúster o modificarlos o acceder a datos confidenciales. Siguiendo las mejores prácticas de seguridad, AWS recomienda restringir el acceso al punto final del clúster de EKS únicamente a los rangos de IP necesarios.

Modifique el acceso al punto final

En la búsqueda de exposición, abra el recurso. Esto abrirá el clúster Amazon EKS afectado. Puede configurar el clúster para que utilice el acceso privado, el acceso público o ambos. Con el acceso privado, las solicitudes de API de Kubernetes que se originan en la VPC de tu clúster utilizan el punto de enlace de la VPC privada. Con el acceso público, las solicitudes de API de Kubernetes que se originan fuera de la VPC del clúster utilizan el punto de enlace público.

Modifica o elimina el acceso público al clúster

Para modificar el acceso al punto de enlace de un clúster existente, consulte [Modificación del acceso al punto de enlace del clúster](#) en la Guía del usuario de Amazon Elastic Kubernetes Service. Implemente reglas más restrictivas basadas en rangos de IP o grupos de seguridad específicos. Si es necesario un acceso público limitado, restrinja el acceso a rangos de bloques del CIDR específicos o utilice listas de prefijos.

El clúster de Amazon EKS utiliza una versión de Kubernetes no compatible

Amazon EKS admite todas las versiones de Kubernetes durante un período de tiempo limitado. La ejecución de clústeres con versiones de Kubernetes no compatibles puede exponer su entorno a vulnerabilidades de seguridad, ya que los parches de CVE dejarán de publicarse para las versiones desactualizadas. Las versiones no compatibles pueden contener vulnerabilidades de seguridad conocidas que pueden ser aprovechadas por los atacantes y carecer de las funciones de seguridad que pueden estar disponibles en las versiones más recientes. Siguiendo las prácticas recomendadas de seguridad, AWS recomienda mantener actualizada la versión de Kubernetes.

Actualización de una versión de Kubernetes

En la búsqueda de exposición, abra el recurso. Esto abrirá el clúster Amazon EKS afectado. Antes de actualizar el clúster, consulte [las versiones disponibles con soporte estándar en](#) la Guía del usuario de Amazon Elastic Kubernetes Service para ver una lista de las versiones de Kubernetes compatibles actualmente.

El clúster de Amazon EKS utiliza secretos de Kubernetes no cifrados

Los secretos de Kubernetes se almacenan, de forma predeterminada, sin cifrar en el almacén de datos subyacente del servidor API (etcd). Cualquier persona con acceso a la API o a etcd puede recuperar o modificar un secreto. Para evitarlo, debes cifrar los secretos de Kubernetes en reposo. Si los secretos de Kubernetes no están cifrados, son vulnerables al acceso no autorizado si etcd se ve comprometido. Dado que los secretos suelen contener información confidencial, como contraseñas y tokens de API, su exposición podría provocar el acceso no autorizado a otras aplicaciones y datos. Siguiendo las prácticas recomendadas de seguridad, AWS recomienda cifrar toda la información confidencial almacenada en los secretos de Kubernetes.

Cifra los secretos de Kubernetes

Amazon EKS admite el cifrado de los secretos de Kubernetes mediante claves de KMS mediante el cifrado de sobres. Para habilitar el cifrado de los secretos de Kubernetes para su clúster de EKS, consulte [Cifrar los secretos de Kubernetes con KMS en los clústeres existentes en](#) la Guía del usuario de Amazon EKS.

Características de vulnerabilidad de los clústeres de Amazon EKS

Estas son las características de vulnerabilidad de los clústeres de Amazon EKS.

El clúster Amazon EKS tiene un contenedor con vulnerabilidades de software explotables en red con una alta probabilidad de explotación

Los paquetes de software que están instalados en los clústeres de EKS pueden estar expuestos a vulnerabilidades y exposiciones comunes (CWEs). Las críticas CVEs representan riesgos de seguridad importantes para su AWS entorno. Los usuarios no autorizados pueden aprovechar estas vulnerabilidades no corregidas para comprometer la confidencialidad, la integridad o la disponibilidad de los datos, o para acceder a otros sistemas. Las vulnerabilidades críticas con una alta probabilidad de explotación representan amenazas inmediatas para la seguridad, ya que es posible que los atacantes o las herramientas de escaneo automatizadas ya estén disponibles públicamente y que los atacantes o las herramientas de escaneo automatizadas lo utilicen activamente. Siguiendo las prácticas recomendadas de seguridad, AWS recomienda parchear estas vulnerabilidades para proteger la instancia de los ataques.

Actualiza las instancias afectadas

Actualice las imágenes de sus contenedores a versiones más recientes que incluyan correcciones de seguridad para las vulnerabilidades identificadas. Por lo general, esto implica reconstruir las

imágenes del contenedor con imágenes base o dependencias actualizadas y, a continuación, implementar las nuevas imágenes en el clúster de Amazon EKS.

El clúster Amazon EKS tiene un contenedor con vulnerabilidades de software

Los paquetes de software que se instalan en los clústeres de Amazon EKS pueden estar expuestos a vulnerabilidades y exposiciones comunes (CVEs). Los no críticos CVEs representan debilidades de seguridad con menor gravedad o capacidad de explotación en comparación con los críticos. CVEs Si bien estas vulnerabilidades representan un riesgo menos inmediato, los atacantes aún pueden aprovechar estas vulnerabilidades sin parches para comprometer la confidencialidad, la integridad o la disponibilidad de los datos, o para acceder a otros sistemas. Siguiendo las prácticas recomendadas de seguridad, AWS recomienda parchear estas vulnerabilidades para proteger la instancia de los ataques.

Actualiza las instancias afectadas

Actualice las imágenes de sus contenedores a versiones más recientes que incluyan correcciones de seguridad para las vulnerabilidades identificadas. Por lo general, esto implica reconstruir las imágenes del contenedor con imágenes base o dependencias actualizadas y, a continuación, implementar las nuevas imágenes en el clúster de Amazon EKS.

Corregir las exposiciones de los usuarios de IAM

AWS Security Hub puede generar hallazgos de exposición para los usuarios AWS Identity and Access Management (IAM).

En la consola de Security Hub, el usuario de IAM implicado en una búsqueda de exposición y su información de identificación aparecen en la sección Recursos de los detalles de la búsqueda. De forma programática, puede recuperar los detalles de los recursos con el [GetFindingsV2](#) funcionamiento de la API Security Hub.

Tras identificar el recurso implicado en la detección de una exposición, puede eliminarlo si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus AWS costes. Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de característica.

Un único hallazgo de exposición contiene los problemas identificados en varios temas de remediación. Por el contrario, puede abordar un hallazgo de exposición y reducir su nivel de gravedad abordando solo un tema de remediación. Su enfoque de la remediación de riesgos depende de los requisitos y las cargas de trabajo de su organización.

 Note

La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros recursos. AWS

Las prácticas recomendadas de IAM recomiendan crear funciones de IAM o utilizar la federación con un proveedor de identidades para acceder AWS mediante credenciales temporales en lugar de crear usuarios de IAM individuales. Si esa es una opción para su organización y caso de uso, le recomendamos que cambie a funciones o federaciones en lugar de utilizar usuarios de IAM. Para obtener más información, consulte [Usuarios de IAM](#) en la Guía del usuario de IAM.

Contenido

- [Características de mala configuración para los usuarios de IAM](#)
 - [El usuario de IAM tiene una política con acceso administrativo](#)
 - [El usuario de IAM no tiene habilitada la MFA](#)
 - [El usuario de IAM tiene una política con acceso administrativo a un Servicio de AWS](#)
 - [La AWS cuenta del usuario de IAM tiene políticas de contraseñas poco seguras](#)
 - [El usuario de IAM tiene credenciales sin utilizar](#)
 - [El usuario de IAM tiene claves de acceso no rotadas](#)
 - [El usuario de IAM tiene una política que permite el acceso sin restricciones al descifrado de claves de KMS](#)

Características de mala configuración para los usuarios de IAM

Estas son las características de los errores de configuración para los usuarios de IAM y las medidas de corrección sugeridas.

El usuario de IAM tiene una política con acceso administrativo

Las políticas de IAM otorgan un conjunto de privilegios a los usuarios de IAM cuando acceden a los recursos. Las políticas administrativas proporcionan a los usuarios de IAM amplios permisos para acceder a los AWS servicios y recursos. Proporcionar todos los privilegios administrativos, en lugar del conjunto mínimo de permisos que el usuario necesita, puede aumentar el alcance de un ataque si las credenciales se ven comprometidas. Siguiendo los principios de seguridad estándar, se AWS

recomienda conceder el mínimo de privilegios, lo que significa que se concedan únicamente los permisos necesarios para realizar una tarea.

1. Revise e identifique las políticas administrativas: en el ID del recurso, identifique el nombre del rol de IAM. Ve al panel de control de IAM y selecciona el rol identificado. Revise la política de permisos adjunta al usuario de IAM. Si la política es una política AWS gestionada, busque `AdministratorAccess` o `IAMFullAccess`. De lo contrario, en el documento de política, busque las declaraciones que tengan `"Effect": "Allow"` un `"Action": "*" asterisco "Resource": "*" "`.
2. Implemente el acceso con privilegios mínimos: sustituya las políticas administrativas del servicio por aquellas que concedan únicamente los permisos específicos necesarios para que el usuario pueda funcionar. Para obtener más información sobre las prácticas recomendadas de seguridad para las políticas de IAM, consulte [Aplicar permisos con privilegios mínimos](#) en la Guía del usuario. AWS Identity and Access Management. Para identificar los permisos innecesarios, puede utilizar el analizador de acceso de IAM para saber cómo modificar su política en función del historial de acceso. Para obtener más información, consulte las [conclusiones sobre el acceso externo y no utilizado](#) en la Guía del AWS Identity and Access Management usuario.
3. Consideraciones de configuración segura: si se necesitan permisos administrativos del servicio para la instancia, considere la posibilidad de implementar estos controles de seguridad adicionales para mitigar el riesgo:
 - Autenticación multifactor (MFA): la MFA agrega una capa de seguridad adicional al requerir una forma de autenticación adicional. Esto ayuda a evitar el acceso no autorizado incluso si las credenciales están comprometidas. Para obtener más información, consulte [Requerir la autenticación multifactor \(MFA\)](#) en AWS Identity and Access Management la Guía del usuario.
 - Condiciones de IAM: la configuración de los elementos de condición le permite restringir cuándo y cómo se pueden usar los permisos administrativos en función de factores como la IP de origen o la antigüedad del MFA. Para obtener más información, consulte [las condiciones de uso en las políticas de IAM](#) para restringir aún más el acceso en la Guía del AWS Identity and Access Management usuario.
 - Límites de permisos: los límites de permisos establecen el número máximo de permisos que puede tener un rol y proporcionan barreras a los roles con acceso administrativo. Para obtener más información, consulte [Usar los límites de permisos para delegar la administración de permisos dentro de una cuenta](#) en la Guía del AWS Identity and Access Management usuario.

El usuario de IAM no tiene habilitada la MFA

La autenticación multifactor (MFA) agrega una capa adicional de protección además del nombre de usuario y la contraseña. Cuando la MFA está habilitada y un usuario de IAM inicia sesión en un AWS sitio web, se le solicita su nombre de usuario, contraseña y un código de autenticación de su dispositivo de AWS MFA. La entidad de autenticación debe poseer un dispositivo que emita una clave sujeta a limitación temporal y debe tener conocimiento de una credencial. Sin la MFA, si la contraseña de un usuario se ve comprometida, el atacante obtiene acceso total a los permisos del AWS usuario. Siguiendo los principios de seguridad estándar, AWS recomienda habilitar la MFA para todas las cuentas y usuarios que tengan AWS Management Console acceso.

Revise los tipos de MFA

AWS admite los siguientes tipos [de MFA](#):

- Claves de acceso y claves de seguridad
- Aplicaciones de autenticador virtual
- Tokens TOTP físicos

Si bien la autenticación con un dispositivo físico suele ofrecer una protección de seguridad más estricta, utilizar cualquier tipo de MFA es más seguro que desactivarla.

Habilitar MFA

Para habilitar el tipo de MFA que se adapte a sus necesidades, consulte la [autenticación AWS multifactorial en IAM en la Guía del usuario de IAM](#). Siga los pasos correspondientes al tipo de MFA específico que desee implementar. Para las organizaciones que administran muchos usuarios, es posible que desee imponer el uso de MFA exigiendo que MFA acceda a recursos confidenciales.

El usuario de IAM tiene una política con acceso administrativo a un Servicio de AWS

Las políticas de administración del servicio proporcionan a los usuarios de IAM permisos para realizar todas las acciones dentro de un servicio específico AWS . Estas políticas suelen incluir permisos que no son necesarios para que los usuarios desempeñen sus funciones laborales. Proporcionar a un usuario de IAM privilegios de administrador de servicios, en lugar del conjunto mínimo de permisos necesario, aumenta el alcance de un ataque si las credenciales se ven comprometidas. Siguiendo los principios de seguridad estándar, se AWS recomienda conceder los privilegios mínimos, es decir, conceder únicamente los permisos necesarios para realizar una tarea.

Revise e identifique las políticas de administración del servicio

En el ID de recurso, identifique el nombre del rol de IAM. Vaya al panel de control de IAM y seleccione el rol identificado. Revise la política de permisos adjunta al usuario de IAM. Si la política es una política gestionada por AWS, busque `AdministratorAccess` o `IAMFullAccess`. De lo contrario, en el documento de política, busque las declaraciones que contengan las declaraciones `"Effect": "Allow" with "Action": "*" over "Resource": "*".`

Implementación del acceso a los privilegios mínimos

Sustituya las políticas administrativas del servicio por aquellas que concedan únicamente los permisos específicos necesarios para que el usuario pueda funcionar. Para identificar los permisos innecesarios, puede utilizar el analizador de acceso de IAM para saber cómo modificar su política en función del historial de acceso.

Consideraciones sobre la configuración segura

Si se necesitan permisos administrativos del servicio para la instancia, considere la posibilidad de implementar estos controles de seguridad adicionales para mitigar la exposición:

- La MFA añade una capa de seguridad adicional al requerir una forma adicional de autenticación. Esto ayuda a evitar el acceso no autorizado incluso si las credenciales están comprometidas.
- Utilice elementos de condición para restringir cuándo y cómo se pueden usar los permisos administrativos en función de factores como la IP de origen o la antigüedad del MFA.
- Usa los límites de permisos para establecer el número máximo de permisos que puede tener un rol, proporcionando barreras para los roles con acceso administrativo.

La AWS cuenta del usuario de IAM tiene políticas de contraseñas poco seguras

Las políticas de contraseñas ayudan a proteger contra el acceso no autorizado al imponer requisitos mínimos de complejidad para las contraseñas de los usuarios de IAM. Sin políticas de contraseñas seguras, aumenta el riesgo de que las cuentas de los usuarios se vean comprometidas a través de ataques de fuerza bruta o adivinación de contraseñas. Siguiendo los principios de seguridad estándar, AWS recomienda implementar una política de contraseñas segura para garantizar que los usuarios creen contraseñas complejas que sean difíciles de adivinar.

Configure una política de contraseñas segura

Ve al panel de control de IAM y dirígete a la configuración de la cuenta. Revisa la configuración actual de la política de contraseñas de tu cuenta, incluida la longitud mínima, los tipos de caracteres requeridos y la configuración de caducidad de las contraseñas.

Como mínimo, AWS recomienda seguir estas prácticas recomendadas al configurar la política de contraseñas:

- Requiere al menos un carácter en mayúscula.
- Requiere al menos un carácter en minúscula.
- Requiere al menos un símbolo.
- Requiere al menos un número.
- Requiere al menos ocho caracteres.

Consideraciones adicionales de seguridad

Tenga en cuenta estas medidas de seguridad adicionales además de una política de contraseñas segura:

- La MFA añade una capa de seguridad adicional al requerir una forma adicional de autenticación. Esto ayuda a evitar el acceso no autorizado incluso si las credenciales están comprometidas.
- Configurar elementos de condición para restringir cuándo y cómo se pueden usar los permisos administrativos en función de factores como la IP de origen o la antigüedad del MFA.

El usuario de IAM tiene credenciales sin utilizar

Las credenciales no utilizadas, incluidas las contraseñas y las claves de acceso que hayan permanecido inactivas durante 90 días o más, representan un riesgo de seguridad para su AWS entorno. Estas credenciales no utilizadas crean posibles vectores de ataque para los atacantes y aumentan la superficie de ataque general de su organización. Siguiendo las mejores prácticas de seguridad, AWS recomienda desactivar o eliminar las credenciales que no se hayan utilizado durante 90 días o más para reducir la superficie de ataque.

Desactiva o elimina las credenciales no utilizadas

En la búsqueda de exposición, abra el recurso. Esto abrirá la ventana de detalles del usuario. Antes de tomar medidas con respecto a las credenciales no utilizadas, evalúe el posible impacto en su entorno. Eliminar las credenciales sin una evaluación adecuada podría interrumpir los procesos en segundo plano, las tareas programadas y más. Considere la posibilidad de pasar un breve período de desactivación antes de eliminarlas definitivamente para comprobar el impacto de eliminar las credenciales no utilizadas.

Tome las medidas adecuadas en función del tipo de credencial:

- En el caso de las contraseñas de consola no utilizadas, considere cambiarla primero y desactivarla temporalmente. Si no surge ningún problema, proceda a la desactivación o eliminación permanente.
- En el caso de las claves de acceso no utilizadas, considere desactivar primero la clave. Tras confirmar que ningún sistema está afectado, proceda a la desactivación o eliminación permanente.
- En el caso de los usuarios no utilizados, considere la posibilidad de desactivarlos temporalmente adjuntando una política restrictiva antes de eliminarlos por completo.

El usuario de IAM tiene claves de acceso no rotadas

Las claves de acceso constan de un identificador de clave de acceso y una clave de acceso secreta que permiten el acceso programático a los recursos. AWS Cuando las claves de acceso permanecen inalteradas durante períodos prolongados, aumentan el riesgo de acceso no autorizado si se ven comprometidas. Siguiendo las mejores prácticas de seguridad, AWS recomienda rotar las claves de acceso cada 90 días para minimizar las oportunidades de que los atacantes utilicen credenciales comprometidas.

Gire las claves de acceso

En la búsqueda de exposición, abra el recurso. Esto abrirá la ventana de detalles del usuario. Para rotar las claves de acceso, consulte [Administrar las claves de acceso para los usuarios de IAM](#) en la Guía del usuario de IAM.

El usuario de IAM tiene una política que permite el acceso sin restricciones al descifrado de claves de KMS

AWS KMS le permite crear y administrar las claves criptográficas que se utilizan para proteger sus datos. Las políticas de IAM que permiten permisos de AWS KMS descifrado ilimitados (por ejemplo, `kms:Decrypt` o `kms:ReEncryptFrom`) sobre todas las claves de KMS pueden provocar el acceso no autorizado a los datos si las credenciales de un usuario de IAM se ven comprometidas. Si un atacante obtiene acceso a estas credenciales, podría descifrar cualquier dato cifrado de su entorno, que podría incluir datos confidenciales. Siguiendo las prácticas recomendadas de seguridad, AWS recomienda implementar el privilegio mínimo limitando los permisos de AWS KMS descifrado únicamente a las claves específicas que los usuarios necesitan para sus funciones laborales.

Implementación del acceso a los privilegios mínimos

En la búsqueda de exposición, abra el recurso. Esto abrirá la ventana Política de IAM. Busque permisos en KMS que permitan `kms:desencriptar` `kms:ReEncryptFrom` o `KMS:*` con una

especificación de recurso de. "*" Actualice la política para restringir los permisos AWS KMS de descifrado únicamente a las claves específicas necesarias. Modifique la política para reemplazar el "*" recurso por la AWS KMS clave específica ARNs requerida.

Consideraciones sobre la configuración segura

Considere la posibilidad de añadir condiciones para restringir aún más el uso de estos permisos. Por ejemplo, puede limitar las operaciones de descifrado a puntos finales de VPC específicos o rangos de IP de origen. También puedes configurar políticas clave para restringir aún más quién puede usar claves de KMS específicas.

Corregir las exposiciones de las funciones Lambda

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

AWS Security Hub puede generar hallazgos de exposición para AWS Lambda funciones (Lambda).

En la consola de Security Hub, la función Lambda implicada en la detección de una exposición y su información de identificación aparecen en la sección Recursos de los detalles de la búsqueda. De forma programática, puede recuperar los detalles de los recursos con el [GetFindingsV2](#) funcionamiento de la API Security Hub.

Tras identificar el recurso implicado en la detección de una exposición, puede eliminarlo si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus AWS costes. Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de característica.

Un único hallazgo de exposición contiene los problemas identificados en varios temas de remediación. Por el contrario, puede abordar un hallazgo de exposición y reducir su nivel de gravedad abordando solo un tema de remediación. Su enfoque de la remediación de riesgos depende de los requisitos y las cargas de trabajo de su organización.

Note

La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros recursos. AWS

 Note

La guía de remediación proporcionada en este tema puede requerir consultas adicionales en otros AWS recursos.

Contenido

- [Características de mala configuración de las funciones Lambda](#)
 - [La función Lambda ejecuta un tiempo de ejecución no compatible](#)
 - [La función Lambda se implementa fuera de una Amazon VPC](#)
 - [La función Lambda puede asumir una función de IAM](#)
 - [El rol de IAM asociado a la función Lambda tiene una política de acceso administrativo](#)
 - [El rol de IAM asociado a la función Lambda tiene una política con acceso administrativo a un servicio AWS](#)
- [Características de accesibilidad de las funciones Lambda](#)
 - [La función Lambda se puede invocar públicamente](#)
- [Características de vulnerabilidad de las funciones Lambda](#)
 - [La función Lambda tiene vulnerabilidades de software que pueden explotarse en la red](#)
 - [La función Lambda tiene vulnerabilidades de software](#)

Características de mala configuración de las funciones Lambda

Estas son las características de configuración errónea de las funciones de Lambda y las medidas de corrección sugeridas.

La función Lambda ejecuta un tiempo de ejecución no compatible

Lambda permite a los desarrolladores ejecutar código sin aprovisionar ni administrar servidores mediante tiempos de ejecución que ejecutan el código en un entorno gestionado. Lambda aplica automáticamente parches y actualizaciones de seguridad a los tiempos de ejecución gestionados y a sus correspondientes imágenes base de contenedores. Cuando una versión en tiempo de ejecución deja de ser compatible, deja de recibir actualizaciones de seguridad, correcciones de errores o asistencia técnica. Las funciones que se ejecutan en tiempos de ejecución obsoletos pueden tener vulnerabilidades de seguridad y, con el tiempo, pueden dejar de funcionar debido a problemas como la caducidad del certificado. Además, los tiempos de ejecución no compatibles pueden ser

vulnerables a vulnerabilidades de seguridad recién descubiertas si no hay parches disponibles. Siguiendo las prácticas recomendadas de seguridad, recomendamos utilizar tiempos de ejecución parcheados y compatibles para las funciones de Lambda.

Actualice el tiempo de ejecución de

En la pestaña Recursos de la exposición, abra el recurso con el hipervínculo. Esto abrirá la ventana de la función Lambda. Para actualizar la función a un entorno de ejecución compatible, configure la configuración de administración del tiempo de ejecución. Puede elegir que la función se actualice automáticamente a la última versión en tiempo de ejecución, pero antes de seleccionar esta opción, evalúe si las actualizaciones automáticas podrían afectar a las aplicaciones en ejecución. Para obtener más información, consulte [Descripción de cómo Lambda gestiona las actualizaciones de las versiones en tiempo de ejecución](#).

La función Lambda se implementa fuera de una Amazon VPC

Las funciones Lambda se implementan de forma predeterminada con acceso a la Internet pública. Esta configuración predeterminada proporciona a las funciones de Lambda la capacidad de llegar a puntos finales de AWS servicio y externos APIs, pero también las expone a posibles riesgos de seguridad. Las funciones con acceso a Internet podrían utilizarse para filtrar datos, comunicarse con servidores no autorizados o convertirse en puntos de entrada para actores externos si se ven comprometidas. Amazon VPC proporciona aislamiento de red al restringir las funciones de Lambda para que se comuniquen únicamente con los recursos de la red privada definida. Siguiendo los principios de seguridad estándar, recomendamos implementar funciones Lambda en una VPC para mejorar la seguridad mediante el aislamiento de la red.

Adjuntar la función a la VPC

En la búsqueda de exposición, abra el recurso con el hipervínculo. Esto abrirá la ventana de la función Lambda. Para proteger su función Lambda restringiendo su acceso a la red, conéctela a una VPC que cuente con los controles de red adecuados. Antes de adjuntar la función a una VPC, planifique AWS cualquier acceso al servicio que pueda necesitar, ya que las funciones de las subredes privadas sin puertas de enlace NAT o puntos de enlace de la VPC no podrán acceder al servicio. AWS APIs Para obtener información sobre cómo adjuntar una función de Lambda a una Amazon VPC de su cuenta, consulte [Adjuntar funciones de Lambda a una Amazon VPC](#) de su cuenta. Cuenta de AWS Considere la posibilidad de utilizar puntos finales de VPC para la conectividad del servicio sin acceso a Internet si su función requiere acceder a AWS los servicios desde una subred privada. Configure una puerta de enlace NAT si necesita conectividad a Internet saliente desde subredes privadas.

La función Lambda puede asumir una función de IAM

Las funciones Lambda utilizan funciones de IAM para interactuar con los servicios. AWS Estas funciones otorgan permisos a la función Lambda para acceder a AWS los recursos durante la ejecución. Si bien estas funciones a veces son necesarias para que las funciones de Lambda realicen sus tareas, estas funciones deben seguir el principio de privilegios mínimos. Siguiendo los principios de seguridad estándar, AWS recomienda comprobar si los permisos asociados a la función son adecuados en función de la funcionalidad prevista de la función.

1. Determine si se requiere el rol de IAM asociado

Determine si la función Lambda requiere que se configure una función de ejecución de IAM. La mayoría de las funciones de Lambda necesitan permisos básicos para funcionar, como escribir registros en CloudWatch. Revise los permisos asociados a la función de ejecución de la función y determine si la función requiere la función de IAM. Para obtener información sobre las funciones de ejecución de Lambda, consulte Definición de [permisos de funciones de Lambda con una función de ejecución en la Guía para desarrolladores](#). AWS Lambda

2. Implementación del acceso a los privilegios mínimos

Sustituya las políticas excesivamente permisivas por aquellas que concedan únicamente los permisos específicos necesarios para que la función funcione. Para obtener información sobre las mejores prácticas de seguridad para las funciones de IAM, consulte [Aplicar permisos con privilegios mínimos en la Guía del usuario](#). AWS Identity and Access Management Para identificar los permisos innecesarios, puede utilizar el analizador de acceso de IAM para saber cómo modificar su política en función del historial de acceso. Para obtener más información, consulte las [conclusiones sobre el acceso externo y no utilizado](#) en la Guía del AWS Identity and Access Management usuario. Como alternativa, puede crear una nueva función de IAM para evitar que afecte a otras funciones de Lambda que utilizan la función existente. En este escenario, cree una nueva función de IAM y, a continuación, asocie la nueva función de IAM a la instancia. Para obtener instrucciones sobre cómo sustituir un rol de IAM por una función, consulte [Actualizar el rol de ejecución de una función](#) en la AWS Lambda Guía para desarrolladores.

El rol de IAM asociado a la función Lambda tiene una política de acceso administrativo

Las políticas de acceso administrativo proporcionan a las funciones de Lambda amplios permisos para los AWS servicios y recursos. Estas políticas suelen incluir permisos que no son necesarios para la funcionalidad. Proporcionar una identidad de IAM con una política de acceso administrativo en una función de Lambda, en lugar del conjunto mínimo de permisos que necesita la función de

ejecución, puede aumentar el alcance de un ataque si la función se ve comprometida. Siguiendo los principios de seguridad estándar, se AWS recomienda conceder el mínimo de privilegios, lo que significa que se concedan únicamente los permisos necesarios para realizar una tarea.

1. Revise e identifique las políticas administrativas

En la evaluación de la exposición, identifique el nombre de la función. Vaya al panel de control de IAM y busque el rol con el nombre del rol identificado anteriormente. Revise la política de permisos asociada a la función de IAM. Si la política es una política AWS gestionada, busque `AdministratorAccess` o `IAMFullAccess`. De lo contrario, en el documento de política, busque las declaraciones que contengan las declaraciones `"Effect": "Allow"`, `"Action": "*" y "Resource": "*" juntas.`

2. Implementación del acceso a los privilegios mínimos

Sustituya las políticas administrativas por aquellas que concedan únicamente los permisos específicos necesarios para que la función funcione. Para obtener más información sobre las prácticas recomendadas de seguridad para las funciones de IAM, consulte [Aplicar permisos con privilegios mínimos](#) en la Guía del usuario.AWS Identity and Access Management Para identificar los permisos innecesarios, puede utilizar el analizador de acceso de IAM para saber cómo modificar su política en función del historial de acceso. Para obtener más información, consulte las [conclusiones sobre el acceso externo y no utilizado](#) en la Guía del AWS Identity and Access Management usuario. Como alternativa, puede crear una nueva función de IAM para evitar que afecte a otras funciones de Lambda que utilicen la función existente. En este escenario, cree un nuevo rol de IAM. A continuación, asocie el nuevo rol a la instancia. Para obtener información sobre cómo sustituir un rol de IAM por una función, consulte [Actualizar el rol de ejecución de una función](#) en la Guía para AWS Lambda desarrolladores.

3. Consideraciones sobre la configuración segura

Si se necesitan permisos de acceso administrativo para la instancia, considere la posibilidad de implementar estos controles de seguridad adicionales para mitigar el riesgo:

- Autenticación multifactor (MFA): la MFA agrega una capa de seguridad adicional al requerir una forma de autenticación adicional. Esto ayuda a evitar el acceso no autorizado incluso si las credenciales están comprometidas. Para obtener más información, consulte [Requerir la autenticación multifactor \(MFA\)](#) en AWS Identity and Access Management la Guía del usuario.
- Condiciones de IAM: la configuración de los elementos de condición le permite restringir cuándo y cómo se pueden usar los permisos administrativos en función de factores como la IP de origen

o la antigüedad del MFA. Para obtener más información, consulte [las condiciones de uso en las políticas de IAM para restringir aún más el acceso](#) en la Guía del usuario de IAM.

- Límites de permisos: los límites de permisos establecen el número máximo de permisos que puede tener un rol y proporcionan barreras a los roles con acceso administrativo. Para obtener más información, consulte [Usar los límites de permisos para delegar la administración de permisos dentro de una cuenta](#) en la Guía del AWS Identity and Access Management usuario.

El rol de IAM asociado a la función Lambda tiene una política con acceso administrativo a un servicio AWS

Las políticas de administración de servicios permiten a las funciones de Lambda realizar todas las acciones dentro de un servicio específico AWS . Estas políticas suelen conceder más permisos de los necesarios para el funcionamiento de una función. Si una función de Lambda con una política de administración de servicios se ve comprometida, un atacante podría usar esos permisos para acceder o modificar datos o servicios confidenciales de su AWS entorno. Siguiendo los principios de seguridad estándar, le recomendamos que conceda los privilegios mínimos, es decir, que conceda únicamente los permisos necesarios para realizar una tarea.

1. Revise e identifique las políticas administrativas

En el hallazgo de exposición, identifique el nombre de la función en el ARN. Ve al panel de control de IAM y busca el nombre del rol. Revise la política de permisos adjunta al rol. Si la política es una política AWS administrada, busque `AdministratorAccess` o `IAMFullAccess`. De lo contrario, en el documento de política, busque las declaraciones que contengan las declaraciones `"Effect": "Allow"`, `"Action": "*" y "Resource": "*"`.

2. Implementación del acceso a los privilegios mínimos

Sustituya las políticas administrativas por aquellas que concedan únicamente los permisos específicos necesarios para que la función funcione. Para obtener más información, consulte [Aplicar permisos de privilegio mínimo](#) en la Guía del usuario de AWS Identity and Access Management . Para identificar los permisos innecesarios, puede utilizar el analizador de acceso de IAM para saber cómo modificar su política en función del historial de acceso. Para obtener más información, consulte las [conclusiones sobre el acceso externo y no utilizado](#) en la Guía del AWS Identity and Access Management usuario. Como alternativa, puede crear una nueva función de IAM para evitar que afecte a otras funciones de Lambda que utilizan la función existente. En este escenario, cree una nueva función de IAM y, a continuación, asocie la nueva función de IAM a la

instancia. Para obtener instrucciones sobre cómo sustituir un rol de IAM por una función, consulte [Actualizar el rol de ejecución de una función](#) en la AWS Lambda Guía para desarrolladores.

3. Consideraciones sobre la configuración segura

Si se necesitan permisos administrativos de nivel de servicio para la instancia, considere la posibilidad de implementar estos controles de seguridad adicionales para mitigar el riesgo:

- Autenticación multifactor (MFA): la MFA agrega una capa de seguridad adicional al requerir una forma de autenticación adicional. Esto ayuda a evitar el acceso no autorizado incluso si las credenciales están comprometidas. Para obtener más información, consulte [Requerir la autenticación multifactor \(MFA\)](#) en AWS Identity and Access Management la Guía del usuario.
- Condiciones de IAM: la configuración de los elementos de condición le permite restringir cuándo y cómo se pueden usar los permisos administrativos en función de factores como la IP de origen o la antigüedad del MFA. Para obtener más información, consulte [las condiciones de uso en las políticas de IAM para restringir aún más el acceso](#) en la Guía del AWS Identity and Access Management usuario.
- Límites de permisos: los límites de los permisos establecen el número máximo de permisos que puede tener un rol y proporcionan barreras a los roles con acceso administrativo. Para obtener más información, consulte [Usar los límites de permisos para delegar la administración de permisos](#) en la Guía del AWS Identity and Access Management usuario.

Características de accesibilidad de las funciones Lambda

Estas son las características de accesibilidad de las funciones Lambda y las medidas de corrección sugeridas.

La función Lambda se puede invocar públicamente

Las políticas de Lambda basadas en recursos determinan quién puede invocar sus funciones. Una función con una política de recursos que incluya «*» como elemento principal (o ningún elemento principal) permite que cualquier usuario autenticado AWS la invoque. Esto supone un riesgo importante, especialmente para las funciones que procesan datos confidenciales, modifican recursos o tienen permisos elevados. Los usuarios no autorizados podrían aprovechar esta configuración para realizar operaciones no deseadas, lo que podría exponer datos, manipular recursos o abusar de las capacidades de las funciones. Siguiendo las mejores prácticas de seguridad, recomendamos restringir el acceso a las funciones Lambda únicamente a los directores autorizados.

Modifique la política basada en los recursos de la función

En la pestaña Recursos de la exposición, abra el recurso con el hipervínculo. Esto abrirá la ventana de la función Lambda. Restrinja el acceso a su función Lambda especificando solo la AWS cuenta autorizada IDs o los principales de IAM específicos (usuarios, funciones o servicios) en la política basada en recursos. Solo puede modificar las políticas basadas en recursos mediante programación.

Características de vulnerabilidad de las funciones Lambda

Estos son los rasgos de vulnerabilidad de las funciones Lambda y las medidas de corrección sugeridas.

La función Lambda tiene vulnerabilidades de software que pueden explotarse en la red

Los paquetes de software utilizados en el código de función Lambda pueden contener vulnerabilidades y exposiciones comunes (CVEs) que tienen una alta probabilidad de ser explotadas. Las críticas CVEs representan riesgos de seguridad importantes para su entorno. AWS Los atacantes pueden aprovechar las vulnerabilidades no parcheadas y poner en riesgo la confidencialidad, integridad o disponibilidad de los datos, así como acceder a otros sistemas. Las vulnerabilidades críticas con una alta probabilidad de explotación representan amenazas inmediatas para la seguridad, ya que es posible que el código de vulnerabilidad ya esté disponible públicamente y los atacantes o las herramientas de escaneo automatizadas lo utilicen activamente. Siguiendo las mejores prácticas de seguridad, te recomendamos corregir estas vulnerabilidades para proteger tu función de los ataques.

Actualiza las funciones afectadas

Consulta la sección Referencias de la pestaña Vulnerabilidad para ver la característica. La documentación del proveedor puede incluir una guía de remediación específica. Actualice las bibliotecas vulnerables a sus últimas versiones seguras siguiendo los procedimientos recomendados por el proveedor. Por lo general, el flujo de trabajo de corrección depende de si implementó el paquete Lambda cargando un archivo zip o creando una función Lambda con una imagen de contenedor. Tras actualizar las bibliotecas, actualice el código de la función Lambda para utilizar la versión fija. Después, implemente la versión actualizada.

La función Lambda tiene vulnerabilidades de software

Las funciones Lambda suelen utilizar bibliotecas y dependencias de terceros que pueden contener vulnerabilidades de seguridad con menor gravedad o capacidad de explotación en comparación con las críticas. CVEs Si bien es posible que estas vulnerabilidades no críticas no se puedan explotar de forma tan inmediata, siguen representando debilidades de seguridad que podrían combinarse

con otras vulnerabilidades y comprometer su funcionamiento. Con el tiempo, también podrían surgir nuevas técnicas de explotación que aumenten el riesgo de estas vulnerabilidades. Siguiendo los principios de seguridad estándar, recomendamos parchear estas vulnerabilidades para mantener un entorno seguro.

Consulte la sección de referencias de la pestaña Vulnerabilidad para ver la característica. La documentación del proveedor puede incluir una guía de remediación específica. Actualice las bibliotecas vulnerables a sus últimas versiones seguras siguiendo los procedimientos recomendados por el proveedor. Por lo general, el flujo de trabajo de corrección depende de si implementó el paquete Lambda cargando un archivo zip o creando una función Lambda con una imagen de contenedor. Tras actualizar las bibliotecas, actualice el código de la función Lambda para utilizar la versión fija. Después, implemente la versión actualizada.

Corregir las exposiciones de las funciones de Amazon RDS

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

AWS Security Hub puede generar resultados de exposición para las funciones de Amazon RDS.

En la consola de Security Hub, la función de Amazon RDS implicada en la detección de una exposición y su información de identificación aparecen en la sección Recursos de los detalles de la búsqueda. De forma programática, puede recuperar los detalles de los recursos con el [GetFindingsV2](#) funcionamiento de la API Security Hub.

Tras identificar el recurso implicado en la detección de una exposición, puede eliminarlo si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus AWS costes. Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de característica.

Un único hallazgo de exposición contiene los problemas identificados en varios temas de remediación. Por el contrario, puede abordar un hallazgo de exposición y reducir su nivel de gravedad abordando solo un tema de remediación. Su enfoque de la remediación de riesgos depende de los requisitos y las cargas de trabajo de su organización.

 Note

La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros recursos. AWS

Contenido

- [Características de mala configuración de las funciones de Amazon RDS](#)
 - [La instancia de base de datos de Amazon RDS está configurada con acceso público](#)
 - [El clúster de base de datos de Amazon RDS tiene un snapshost que se comparte públicamente](#)
 - [La instancia de base de datos de Amazon RDS tiene una instantánea que no está cifrada en reposo](#)
 - [El clúster de base de datos de Amazon RDS tiene una instantánea que no está cifrada en reposo](#)
 - [La instancia de base de datos de Amazon RDS tiene un grupo de seguridad abierto](#)
 - [La instancia de base de datos de Amazon RDS tiene deshabilitada la autenticación de base de datos de IAM](#)
 - [La instancia de base de datos de Amazon RDS usa el nombre de usuario de administrador predeterminado](#)
 - [El clúster de base de datos de Amazon RDS usa el nombre de usuario de administrador predeterminado](#)
 - [La instancia de base de datos de Amazon RDS tiene inhabilitadas las actualizaciones automáticas de las versiones secundarias](#)
 - [La instancia de base de datos de Amazon RDS tiene deshabilitadas las copias de seguridad automáticas](#)
 - [La instancia de base de datos de Amazon RDS tiene deshabilitada la protección contra la eliminación](#)
 - [El clúster de base de datos de Amazon RDS tiene deshabilitada la protección contra la eliminación](#)
 - [La instancia de base de datos Amazon RDS usa el puerto predeterminado para el motor de base de datos.](#)
 - [La instancia de base de datos de Amazon RDS no está cubierta por un plan de respaldo](#)

Características de mala configuración de las funciones de Amazon RDS

A continuación, se describen los errores de configuración y los pasos para subsanarlos de las funciones de Amazon RDS.

La instancia de base de datos de Amazon RDS está configurada con acceso público

Es posible que se pueda acceder a las instancias de Amazon RDS con acceso público a través de Internet a través de sus puntos de enlace. Si bien el acceso público a veces es necesario, por ejemplo, para funcionar, esta configuración se puede utilizar como un posible vector de ataque para que usuarios no autorizados intenten acceder a su base de datos. Las bases de datos de acceso público pueden estar expuestas al escaneo de puertos, a ataques de fuerza bruta y a intentos de explotación. Siguiendo los principios de seguridad estándar, le recomendamos que limite la exposición pública de los recursos de su base de datos.

1. Modifique la configuración de acceso público

En la búsqueda de exposición, abra el recurso con el hipervínculo. Esto abrirá la instancia de base de datos afectada. Evalúe si la instancia de base de datos requiere accesibilidad pública en función de la arquitectura de su aplicación. Para obtener más información, consulte [Configurar el acceso público o privado en Amazon RDS](#).

El clúster de base de datos de Amazon RDS tiene un snapshot que se comparte públicamente

Cualquier persona puede acceder a las instantáneas públicas Cuenta de AWS, lo que podría exponer los datos confidenciales a usuarios no autorizados. Cualquiera Cuenta de AWS tiene permiso para copiar estas instantáneas públicas y crear instancias de base de datos a partir de ellas, lo que podría provocar filtraciones de datos o un acceso no autorizado a los datos. Siguiendo las prácticas recomendadas de seguridad, le recomendamos que restrinja el acceso a sus instantáneas de Amazon RDS únicamente a organizaciones Cuentas de AWS y organizaciones de confianza.

1. Configurar una instantánea de Amazon RDS para acceso privado

En la búsqueda de exposición, abra el recurso a través del hipervínculo. Para obtener información sobre cómo modificar la configuración de uso compartido de instantáneas, consulte [Compartir una instantánea](#) en la Guía del usuario de Amazon Aurora. Para obtener información sobre cómo dejar de compartir instantáneas, consulte [Cómo dejar de compartir instantáneas](#) en la Guía del usuario de Amazon Aurora. .

La instancia de base de datos de Amazon RDS tiene una instantánea que no está cifrada en reposo

Las instantáneas de instancias de base de datos Amazon RDS sin cifrar pueden exponer datos confidenciales si se obtiene un acceso no autorizado a la capa de almacenamiento. Sin el cifrado, los datos de las instantáneas podrían quedar expuestos a causa de un acceso no autorizado. Esto crea un riesgo de filtraciones de datos e infracciones de conformidad. Siguiendo las mejores prácticas de seguridad, recomendamos cifrar todos los recursos de la base de datos y sus copias de seguridad para mantener la confidencialidad de los datos.

En la búsqueda de exposición, abra el recurso con el hipervínculo. Esto abrirá la instantánea afectada. No puede cifrar directamente una instantánea no cifrada existente. En su lugar, cree una copia cifrada de la instantánea no cifrada. Para obtener instrucciones detalladas, consulte [Copia y cifrado de instantáneas de clústeres de bases de datos de recursos de Amazon RDS](#) en la Guía del usuario de Amazon Aurora. ..

El clúster de base de datos de Amazon RDS tiene una instantánea que no está cifrada en reposo

Las instantáneas del clúster de base de datos de Amazon RDS sin cifrar pueden exponer datos confidenciales si se obtiene un acceso no autorizado a la capa de almacenamiento. Sin el cifrado, los datos de las instantáneas podrían quedar expuestos a causa de un acceso no autorizado. Esto crea un riesgo de filtraciones de datos e infracciones de conformidad. Siguiendo las mejores prácticas de seguridad, recomendamos cifrar todos los recursos de la base de datos y sus copias de seguridad para mantener la confidencialidad de los datos.

1. Cree una copia cifrada de la instantánea

En la búsqueda de exposición, abra el recurso con el hipervínculo. Esto abrirá la instantánea afectada. No puede cifrar directamente una instantánea no cifrada existente. En su lugar, cree una copia cifrada de la instantánea no cifrada. Para obtener instrucciones detalladas, consulte [Copia y cifrado de instantáneas de clústeres de bases de datos de recursos de Amazon RDS](#) en la Guía del usuario de Amazon Aurora. ..

La instancia de base de datos de Amazon RDS tiene un grupo de seguridad abierto

Los grupos de seguridad actúan como firewalls virtuales para sus instancias de Amazon RDS a fin de controlar el tráfico entrante y saliente. Los grupos de seguridad abiertos, que permiten el acceso sin restricciones desde cualquier dirección IP, pueden exponer las instancias de su base de datos a accesos no autorizados y a posibles ataques. Siguiendo los principios de seguridad estándar, recomendamos restringir el acceso de los grupos de seguridad a direcciones IP y puertos específicos para mantener el principio de privilegios mínimos.

Revise las reglas de los grupos de seguridad y evalúe la configuración actual

En la búsqueda de exposición, abra el recurso del grupo de seguridad de la instancia de base de datos. Evalúe qué puertos están abiertos y accesibles desde amplios rangos de IP, por ejemplo(0.0.0.0/0 or ::/0). Para obtener información sobre cómo ver los detalles de los grupos de seguridad, consulte [DescribeSecurityGroups](#) la referencia de la API de Amazon Elastic Compute Cloud.

Modifique las reglas de los grupos de seguridad

Modifique las reglas del grupo de seguridad para restringir el acceso a rangos o direcciones IP de confianza específicos. Al actualizar las reglas del grupo de seguridad, considere separar los requisitos de acceso para los distintos segmentos de la red creando reglas para cada rango de IP de origen requerido o restringiendo el acceso a puertos específicos. Para modificar las reglas de los grupos de seguridad, consulte [Configurar las reglas de los grupos de seguridad](#) en la Guía del EC2 usuario de Amazon. Para modificar el puerto predeterminado de una instancia de base de datos de Amazon RDS existente, consulte [Modificación del clúster de base de datos mediante la consola, la CLI y la API](#) en la Guía del usuario de Amazon Aurora.

La instancia de base de datos de Amazon RDS tiene deshabilitada la autenticación de base de datos de IAM

La autenticación de bases de datos de IAM le permite autenticarse en su base de datos de Amazon RDS con credenciales de IAM en lugar de contraseñas de bases de datos. Esto proporciona varios beneficios de seguridad, como la administración centralizada del acceso, las credenciales temporales y la eliminación del almacenamiento de las contraseñas de las bases de datos en el código de la aplicación. La autenticación de bases de datos de IAM permite autenticar las instancias de bases de datos con un token de autenticación en lugar de una contraseña. Como resultado, el tráfico de red que entra y sale de la instancia de base de datos se cifra mediante SSL. Sin la autenticación de IAM, las bases de datos suelen depender de la autenticación basada en contraseñas, lo que puede provocar la reutilización de las contraseñas y las contraseñas no seguras. Siguiendo las prácticas recomendadas de seguridad, recomendamos habilitar la autenticación de bases de datos de IAM.

Habilite la autenticación de bases de datos de IAM

En la búsqueda de exposición, abra el recurso con el hipervínculo. Esto abrirá la instancia de base de datos afectada. Puede habilitar la autenticación de la base de datos de IAM en las opciones de base de datos. Para obtener más información, consulte [Habilitar y deshabilitar la autenticación de](#)

[bases de datos de IAM](#) en la Guía del usuario de Amazon RDS. Tras habilitar la autenticación de IAM, actualice las instancias de base de datos para que utilicen la autenticación de IAM en lugar de la autenticación basada en contraseñas.

La instancia de base de datos de Amazon RDS usa el nombre de usuario de administrador predeterminado

El uso de nombres de usuario predeterminados (p. ej., «admin» o «root») para las instancias de base de datos aumenta el riesgo de seguridad, ya que son ampliamente conocidos y suelen ser objeto de ataques de fuerza bruta. Los nombres de usuario predeterminados son predecibles y facilitan que los usuarios no autorizados intenten acceder a su base de datos. Con los nombres de usuario predeterminados, los atacantes solo necesitan obtener las contraseñas, en lugar de necesitar ambas para acceder a la base de datos. Siguiendo las prácticas recomendadas de seguridad, recomendamos utilizar nombres de usuario de administrador exclusivos para la instancia de base de datos a fin de mejorar la seguridad mediante la ocultación y reducir el riesgo de intentos de acceso no autorizados.

Configure un nombre de usuario de administrador único

En la búsqueda de exposición, abra el recurso con el hipervínculo. Esto abrirá la instancia de base de datos afectada. Considere qué reglas de frecuencia de respaldo, período de retención y ciclo de vida son las mejores para sus aplicaciones.

El clúster de base de datos de Amazon RDS usa el nombre de usuario de administrador predeterminado

El uso de nombres de usuario predeterminados (p. ej., «admin» o «root») para las instancias de base de datos aumenta el riesgo de seguridad, ya que son ampliamente conocidos y suelen ser objeto de ataques de fuerza bruta. Los nombres de usuario predeterminados son predecibles y facilitan que los usuarios no autorizados intenten acceder a su base de datos. Con los nombres de usuario predeterminados, los atacantes solo necesitan obtener las contraseñas, en lugar de necesitar ambas para acceder a la base de datos. Siguiendo las prácticas recomendadas de seguridad, recomendamos utilizar nombres de usuario de administrador exclusivos para la instancia de base de datos a fin de mejorar la seguridad mediante la ocultación y reducir el riesgo de intentos de acceso no autorizados.

Configure un nombre de usuario de administrador único

En la búsqueda de exposición, abra el recurso con el hipervínculo. Esto abrirá la instancia de base de datos afectada. No puede cambiar el nombre de usuario de administrador de una instancia de

base de datos de Amazon RDS existente. Para crear un nombre de administrador único, debe crear una nueva instancia de base de datos con un nombre de usuario personalizado y migrar los datos.

La instancia de base de datos de Amazon RDS tiene inhabilitadas las actualizaciones automáticas de las versiones secundarias

Las actualizaciones automáticas de las versiones secundarias garantizan que sus instancias de Amazon RDS reciban automáticamente las actualizaciones de las versiones secundarias del motor cuando estén disponibles. Estas actualizaciones suelen incluir importantes parches de seguridad y correcciones de errores que ayudan a mantener la seguridad y la estabilidad de la base de datos. Su base de datos corre el riesgo de funcionar con vulnerabilidades de seguridad conocidas que se han corregido en las versiones secundarias más recientes. Sin actualizaciones automáticas, las instancias de bases de datos pueden acumular vulnerabilidades de seguridad a medida que se descubren nuevas. Siguiendo las prácticas recomendadas de seguridad, recomendamos habilitar las actualizaciones automáticas de las versiones secundarias para todas las instancias de Amazon RDS.

Habilite las actualizaciones automáticas de las versiones secundarias

En la búsqueda de exposición, abra el recurso con el hipervínculo. Esto abrirá la instancia de base de datos afectada. Puede ver la configuración automática de las actualizaciones menores en la pestaña Mantenimiento y copias de seguridad. Para obtener más información, consulte [Actualizaciones automáticas de versiones secundarias de Amazon RDS for MySQL](#). También puede configurar el período de mantenimiento para que se produzca durante los períodos de baja actividad de la base de datos.

La instancia de base de datos de Amazon RDS tiene deshabilitadas las copias de seguridad automáticas

Las copias de seguridad automatizadas proporcionan la point-in-time recuperación de sus instancias de Amazon RDS, lo que le permite restaurar la base de datos en cualquier punto del período de retención. Cuando las copias de seguridad automatizadas están deshabilitadas, corre el riesgo de perder datos en caso de eliminarlos de forma malintencionada, dañarlos u otros escenarios de pérdida de datos. En el caso de que se produzcan actividades malintencionadas, como los ataques de ransomware, la eliminación de tablas de bases de datos o la corrupción, la posibilidad de restaurarlas a un punto en el tiempo anterior al incidente reduce el tiempo necesario para recuperarse de un incidente. Siguiendo las mejores prácticas de seguridad, recomendamos habilitar las copias de seguridad automatizadas con un período de retención adecuado para todas las [bases de datos de producción](#).

La instancia de base de datos de Amazon RDS tiene deshabilitada la protección contra la eliminación

La protección contra la eliminación de bases de datos es una función que ayuda a evitar la eliminación de las instancias de la base de datos. Cuando la protección contra la eliminación está deshabilitada, cualquier usuario con permisos suficientes puede eliminar la base de datos, lo que podría provocar la pérdida de datos o el tiempo de inactividad de la aplicación. Los atacantes pueden eliminar su base de datos, lo que provoca la interrupción del servicio, la pérdida de datos y un aumento del tiempo de recuperación. Siguiendo las prácticas recomendadas de seguridad, le recomendamos que habilite la protección contra la eliminación de sus instancias de base de datos de RDS para evitar que se eliminen de forma malintencionada.

Habilite la protección de eliminación para su clúster de base de datos de Amazon RDS

En la búsqueda de exposición, abra el recurso con el hipervínculo. Esto abrirá el clúster de base de datos afectado.

El clúster de base de datos de Amazon RDS tiene deshabilitada la protección contra la eliminación

La protección contra la eliminación de bases de datos es una función que ayuda a evitar la eliminación de las instancias de la base de datos. Cuando la protección contra la eliminación está deshabilitada, cualquier usuario con permisos suficientes puede eliminar la base de datos, lo que podría provocar la pérdida de datos o el tiempo de inactividad de la aplicación. Los atacantes pueden eliminar su base de datos, lo que provoca la interrupción del servicio, la pérdida de datos y un aumento del tiempo de recuperación. Siguiendo las prácticas recomendadas de seguridad, le recomendamos que habilite la protección contra la eliminación de sus clústeres de bases de datos de RDS para evitar que se eliminen de forma malintencionada.

Habilite la protección de eliminación para su clúster de base de datos de Amazon RDS

En la búsqueda de exposición, abra el recurso con el hipervínculo. Esto abrirá el clúster de base de datos afectado.

La instancia de base de datos Amazon RDS usa el puerto predeterminado para el motor de base de datos.

Las instancias de Amazon RDS que utilizan puertos predeterminados para los motores de bases de datos pueden enfrentarse a mayores riesgos de seguridad, ya que estos puertos predeterminados son ampliamente conocidos y suelen ser el objetivo de las herramientas de análisis automatizadas. La modificación de la instancia de base de datos para que utilice puertos no predeterminados añade una capa adicional de seguridad a través de la oscuridad, lo que dificulta que los usuarios no autorizados realicen ataques automatizados o selectivos a su base de datos. Los puertos

predeterminados suelen ser escaneados por personas no autorizadas y pueden provocar que su instancia de base de datos sea atacada. Siguiendo las prácticas recomendadas de seguridad, recomendamos cambiar el puerto predeterminado por un puerto personalizado para reducir el riesgo de ataques automatizados o dirigidos.

En la búsqueda de exposición, abra el recurso con el hipervínculo. Esto abrirá la instancia de base de datos afectada.

Actualice las cadenas de conexión de la aplicación

Tras cambiar el puerto, actualiza todas las aplicaciones y servicios que se conectan a tu instancia de Amazon RDS para que usen el nuevo número de puerto.

La instancia de base de datos de Amazon RDS no está cubierta por un plan de respaldo

AWS Backup es un servicio de respaldo totalmente gestionado que centraliza y automatiza el respaldo de todos los datos. Servicios de AWS Si su instancia de base de datos no está cubierta por un plan de respaldo, corre el riesgo de perder datos en caso de eliminarlos de forma malintencionada, dañarlos u otros escenarios de pérdida de datos. En caso de que se produzcan actividades malintencionadas, como ataques de ransomware, eliminación de tablas de bases de datos o corrupción, la posibilidad de restaurarlas a un punto en el tiempo anterior al incidente reduce el tiempo necesario para recuperarse de un incidente. Siguiendo las prácticas recomendadas de seguridad, recomendamos incluir las instancias de Amazon RDS en un plan de respaldo para garantizar la protección de los datos.

Cree y asigne un plan de respaldo para su instancia de base de datos

En la búsqueda de exposición, abra el recurso con el hipervínculo. Esto abrirá la instancia de base de datos afectada. Considere qué reglas de frecuencia de respaldo, período de retención y ciclo de vida son las mejores para sus aplicaciones.

Corregir las exposiciones de los buckets de Amazon S3

 Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

AWS Security Hub puede generar datos de exposición para los depósitos de Amazon Simple Storage Service (S3).

En la consola de Security Hub, el bucket de Amazon S3 implicado en la detección de una exposición y su información de identificación aparecen en la sección Recursos de los detalles de la búsqueda. De forma programática, puede recuperar los detalles de los recursos con el [GetFindingsV2](#) funcionamiento de la API Security Hub.

Tras identificar el recurso implicado en la detección de una exposición, puede eliminarlo si no lo necesita. Eliminar un recurso no esencial puede reducir su perfil de exposición y sus AWS costes. Si el recurso es esencial, siga estos pasos de remediación recomendados para ayudar a mitigar el riesgo. Los temas de remediación se dividen según el tipo de característica.

Un único hallazgo de exposición contiene los problemas identificados en varios temas de remediación. Por el contrario, puede abordar un hallazgo de exposición y reducir su nivel de gravedad abordando solo un tema de remediación. Su enfoque de la remediación de riesgos depende de los requisitos y las cargas de trabajo de su organización.

 Note

La guía de remediación que se proporciona en este tema puede requerir consultas adicionales en otros recursos. AWS

Contenido

- [Características de mala configuración de los buckets de Amazon S3](#)
 - [El bucket de Amazon S3 tiene el control de versiones deshabilitado](#)
 - [El bucket de Amazon S3 tiene el bloqueo de objetos desactivado](#)
 - [El bucket de Amazon S3 no está cifrado en reposo con AWS KMS claves](#)
 - [La eliminación de la autenticación multifactor \(MFA\) está deshabilitada en un bucket de Amazon S3 versionado](#)
 - [El bucket de Amazon S3 permite a los directores de otras AWS cuentas modificar los permisos del bucket.](#)
- [Características de accesibilidad de los buckets de Amazon S3](#)
 - [El bucket de Amazon S3 tiene acceso público](#)
 - [El bucket de Amazon S3 tiene acceso de lectura público](#)
 - [El bucket de Amazon S3 tiene acceso de escritura](#)
 - [El punto de acceso Amazon S3 tiene habilitada la configuración de acceso público](#)
- [Características de los datos confidenciales de los buckets de Amazon S3](#)

- [Características de los datos confidenciales de los buckets de Amazon S3](#)

Características de mala configuración de los buckets de Amazon S3

A continuación, se indican las características de los errores de configuración de los buckets de Amazon S3 y se sugieren los pasos para corregirlos.

El bucket de Amazon S3 tiene el control de versiones deshabilitado

El control de versiones de Amazon S3 le ayuda a mantener varias variantes de un objeto en el mismo depósito. Cuando el control de versiones está deshabilitado, Amazon S3 almacena solo la versión más reciente de cada objeto, lo que significa que si los objetos se eliminan o sobrescriben de forma accidental o malintencionada, no se pueden recuperar. Los depósitos habilitados para el control de versiones ofrecen protección contra la eliminación accidental, los fallos de las aplicaciones y los incidentes de seguridad, como los ataques de ransomware, en los que podrían producirse modificaciones o eliminaciones no autorizadas de los datos. Siguiendo las prácticas recomendadas de seguridad, recomendamos habilitar el control de versiones para los depósitos que contienen datos importantes que serían difíciles o imposibles de recrear si se perdieran.

1. Habilitar el control de versiones: para habilitar el control de versiones de Amazon S3 en un bucket, consulte [Habilitar el versionado en buckets en la Guía del usuario](#) de Amazon Simple Storage Service. Cuando habilite el control de versiones, considere la posibilidad de implementar reglas de ciclo de vida para administrar el almacenamiento, ya que el control de versiones mantendrá varias copias de los objetos.

El bucket de Amazon S3 tiene el bloqueo de objetos desactivado

Amazon S3 Object Lock proporciona un modelo write-once-read-many (WORM) para los objetos de Amazon S3, lo que impide que se eliminen o sobrescriban durante un período fijo o indefinidamente. Si el bloqueo de objetos está desactivado, sus objetos podrían ser eliminados, modificados o cifrados de forma accidental o malintencionada a causa de un ransomware. El bloqueo de objetos es especialmente importante para cumplir con los requisitos normativos que exigen el almacenamiento inmutable de los datos y para protegerse contra amenazas sofisticadas, como el ransomware, que pueden intentar cifrar los datos. Al habilitar Object Lock, puede aplicar políticas de retención como una capa adicional de protección de datos y crear una estrategia de respaldo inmutable para sus datos críticos. Siguiendo las prácticas recomendadas de seguridad, le recomendamos que active Object Lock para evitar la modificación malintencionada de sus objetos.

1. Ten en cuenta que el bloqueo de objetos solo se puede activar al crear un depósito nuevo, por lo que tendrás que crear uno nuevo con el bloqueo de objetos activado. Para migraciones grandes, considere la posibilidad de utilizar Batch Operations para copiar los objetos al nuevo depósito. Antes de bloquear cualquier objeto, también debe habilitar el control de versiones y el bloqueo de objetos de Amazon S3 en un bucket. Como Object Lock solo se puede activar en depósitos nuevos, tendrá que migrar los datos existentes a un nuevo depósito con Object Lock activado. Configurar el bloqueo de objetos de Amazon S3: para obtener información sobre cómo configurar el bloqueo de objetos en un depósito, consulte [Configuring Amazon S3 Object Lock](#) en la guía del usuario de Amazon Simple Storage Service. Tras configurar Object Lock, elija un modo de retención adecuado en función de su entorno.

El bucket de Amazon S3 no está cifrado en reposo con AWS KMS claves

Amazon S3 aplica el cifrado del lado del servidor con claves administradas de Amazon S3 como nivel de cifrado predeterminado para todos los buckets nuevos. Si bien las claves administradas de Amazon S3 ofrecen una protección de cifrado sólida, no ofrecen el mismo nivel de control de acceso y capacidades de auditoría que AWS Key Management Service las claves. Cuando se utilizan claves de KMS, el acceso a los objetos requiere permisos tanto para el bucket de Amazon S3 como para la clave de KMS que cifró el objeto. Esto es especialmente importante en el caso de los datos confidenciales, en los que se necesita un control pormenorizado sobre quién puede acceder a los objetos cifrados y un registro de auditoría exhaustivo del uso de las claves de cifrado. Siguiendo las prácticas recomendadas de seguridad, recomendamos utilizar claves KMS para cifrar los depósitos que contienen datos confidenciales o para entornos con requisitos de conformidad estrictos.

1. Configurar la clave de bucket de Amazon S3

Para configurar un bucket para usar una clave de bucket de Amazon S3 para nuevos objetos, consulte [Configurar su bucket para usar una clave de bucket de Amazon S3 con SSE-KMS para nuevos objetos](#) en la Guía del usuario de Amazon Simple Storage Service. Para obtener información sobre cómo cifrar un objeto existente, consulte [Cifrar objetos con Amazon S3 Batch Operations](#) en el blog sobre AWS almacenamiento.

Al implementar el AWS KMS cifrado, tenga en cuenta lo siguiente:

- Administración de claves: decida si desea utilizar una clave AWS gestionada o una clave gestionada por el cliente (CMK). CMKs ofrezca a los clientes un control total sobre el ciclo de vida y el uso de sus claves. Para obtener más información sobre la diferencia entre estos dos

tipos de claves, consulte las [claves de AWS KMS](#) en la Guía para AWS Key Management Service desarrolladores.

- Rotación de claves: para medidas de seguridad adicionales, habilite la rotación automática de claves para sus claves de KMS. Para obtener más información, consulte [Habilitar la rotación automática de claves](#) en la Guía para AWS Key Management Service desarrolladores.

La eliminación de la autenticación multifactor (MFA) está deshabilitada en un bucket de Amazon S3 versionado

La eliminación mediante autenticación multifactor (MFA) proporciona un nivel de seguridad adicional para su bucket de Amazon S3. Requiere una autenticación multifactorial para las operaciones destructivas de Amazon S3. Cuando la eliminación de MFA está deshabilitada, los usuarios con los permisos adecuados pueden eliminar permanentemente las versiones de los objetos o suspender el control de versiones en su bucket sin problemas de autenticación adicionales. La activación de la eliminación por MFA ayuda a proteger sus datos contra la eliminación no autorizada o accidental, lo que proporciona una protección mejorada contra los ataques de ransomware, las amenazas internas y los errores operativos. La eliminación con MFA es especialmente útil para los depósitos que contienen datos críticos o sensibles al cumplimiento y que deben protegerse contra la eliminación no autorizada. Siguiendo las prácticas recomendadas de seguridad, le recomendamos que habilite la MFA para sus buckets de Amazon S3.

1. Revise los tipos de MFA

AWS admite los siguientes tipos [de MFA](#). Si bien la autenticación con un dispositivo físico suele ofrecer una protección de seguridad más estricta, utilizar cualquier tipo de MFA es más seguro que desactivarla.

2. Aplique la MFA a nivel de política de recursos

Utilice la clave de `aws:MultiFactorAuthAge` condición de una política de bucket para exigir la MFA para las operaciones confidenciales. Para obtener más información, consulte [Requerir MFA](#) en la Guía del usuario de Amazon Simple Storage Service.

3. Habilitar MFA

Para habilitar la eliminación de MFA, primero asegúrese de que el control de versiones esté habilitado en su bucket de Amazon S3. La eliminación de MFA solo se admite en depósitos que tienen habilitado el control de versiones. Para obtener información sobre cómo habilitar el control de versiones de Amazon S3, consulte [Habilitar el control de versiones en buckets en la Guía](#) del

usuario de Amazon Simple Storage Service. La eliminación de MFA no se puede activar a través de la consola de Amazon S3. Debe utilizar la API de Amazon S3 o la AWS CLI. Para obtener más información, consulte [Configuración de la eliminación de MFA](#) en la Guía del usuario de Amazon Simple Storage Service.

El bucket de Amazon S3 permite a los directores de otras AWS cuentas modificar los permisos del bucket.

Las políticas de bucket de Amazon S3 controlan el acceso a los buckets y objetos. Cuando las políticas de bucket permiten a los directores de otras AWS cuentas modificar los permisos del bucket, los usuarios no autorizados pueden volver a configurar el bucket. Si las credenciales principales externas se ven comprometidas, los usuarios no autorizados pueden hacerse con el control del bucket y provocar filtraciones de datos o interrupciones en el servicio. Siguiendo los principios de seguridad estándar, se AWS recomienda restringir las acciones de administración de permisos únicamente a los directores de confianza.

1. Revise e identifique las políticas de bucket

En la exposición, identifique el bucket de Amazon S3 en el campo ARN. En la consola de Amazon S3, seleccione el bucket y vaya a la pestaña Permissions para revisar la política del bucket. Revise la política de permisos adjunta al bucket. Busca declaraciones de políticas que otorguen acciones similares `s3:PutBucketPolicy`, `s3:PutBucketAcl`, `s3>DeleteBucketPolicy`, `s3:*` o declaraciones de políticas que permitan el acceso a entidades ajenas a tu cuenta, tal y como se indica en la declaración principal.

2. Modifica la política de cupos

Modifica la política de depósitos para eliminar o restringir las acciones concedidas a otras AWS cuentas:

- Elimine las declaraciones de política que otorgan a las cuentas externas acciones de administración de permisos.
- Si se requiere el acceso entre cuentas, sustituya los permisos (`s3:*`) generales por acciones específicas que no incluyan la administración de permisos de los buckets.

Para obtener información sobre la modificación de una política de bucket, consulte [Añadir una política de bucket mediante la consola de Amazon S3](#) en la Guía del usuario de Amazon S3.

Características de accesibilidad de los buckets de Amazon S3

Estas son las características de accesibilidad de los buckets de Amazon S3 y las medidas de corrección sugeridas.

El bucket de Amazon S3 tiene acceso público

De forma predeterminada, los buckets y objetos de Amazon S3 son privados, pero se pueden hacer públicos mediante diversas configuraciones. Si modifica las políticas de bucket, las políticas de puntos de acceso o los permisos de los objetos para permitir el acceso público, corre el riesgo de exponer los datos confidenciales.

1. Evalúe el depósito

Evalúe si su depósito se puede convertir en privado en función de la política organizativa, los requisitos de cumplimiento o la clasificación de los datos. Si no pretendía conceder acceso al bucket al público o a otras personas Cuentas de AWS, siga las instrucciones de corrección restantes.

2. Configura el depósito para que sea privado

Elija una de las siguientes opciones para configurar el acceso privado a su bucket de Amazon S3:

- Nivel de cuenta: para bloquear el acceso público a todos los depósitos de tu cuenta mediante los ajustes a nivel de cuenta, consulta [Configurar los ajustes de bloqueo de acceso público para tu cuenta en la Guía del usuario](#) de Amazon Simple Storage Service.
- Nivel de depósito: para bloquear el acceso público a un depósito específico, consulte [Configuración de los ajustes de bloqueo de acceso público para sus depósitos de Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.
- ACL o políticas del bucket: para modificar la lista de control de acceso (ACL) del bucket, la política del bucket, la política del punto de acceso multirregional (MRAP) o la política del punto de acceso para eliminar el acceso público al bucket, consulte [Revisar y cambiar el acceso al bucket](#) en la Guía del usuario de Amazon Simple Storage Service. Si bloquea el acceso público a nivel de cuenta o de depósito, esos bloqueos tienen prioridad sobre una política que permita el acceso público.

El bucket de Amazon S3 tiene acceso de lectura público

Los buckets de Amazon S3 con acceso público de lectura permiten que cualquier usuario de Internet vea el contenido de su bucket. Si bien esto puede ser necesario para los sitios web de acceso

público o los recursos compartidos, puede generar riesgos de seguridad si el depósito contiene datos confidenciales. El acceso público de lectura puede provocar la visualización y descarga no autorizadas, lo que puede provocar violaciones de datos si se almacenan datos confidenciales en esos depósitos. Siguiendo los principios de seguridad estándar, AWS recomienda restringir el acceso a los buckets de Amazon S3 a los usuarios y sistemas necesarios.

1. Bloquee el acceso público a nivel de bucket

Amazon S3 proporciona ajustes de bloqueo de acceso público que se pueden configurar tanto a nivel de bucket como de cuenta para impedir el acceso público independientemente de las políticas del bucket o ACLs. Para obtener más información, consulte [Bloquear el acceso público a su almacenamiento de Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service. Tras bloquear el acceso público, revise la configuración de control de acceso del bucket para asegurarse de que se ajusta a sus requisitos de acceso. A continuación, revise su política de bucket de Amazon S3 para definir de forma explícita quién puede acceder a su bucket. Para ver ejemplos de políticas de bucket, consulte [Ejemplos de políticas de bucket de Amazon S3 en la Guía del](#) usuario de Amazon Simple Storage Service.

2. Métodos de acceso alternativos

Si se requiere el acceso público de lectura, considere estas alternativas más seguras:

- CloudFront— Úselo CloudFront con una identidad de acceso de origen (OAI) o un control de acceso de origen (OAC) para permitir el acceso de lectura desde un bucket privado de Amazon S3. Esta alternativa restringe el acceso directo a su bucket de Amazon S3 y, al mismo tiempo, permite que el contenido sea accesible públicamente a través CloudFront de él. Para obtener más información, consulte [Restringir el acceso a un origen de Amazon S3](#) en la Guía para CloudFront desarrolladores de Amazon.
- Prefirmado URLs: utilice prefirado URLs para acceder temporalmente a objetos específicos. Para obtener más información, consulte [Compartir objetos con prefirados URLs](#) en la Guía del AWSAmazon usuario de S3.

El bucket de Amazon S3 tiene acceso de escritura

Los buckets de Amazon S3 con acceso de escritura público permiten que cualquier usuario de Internet cargue, modifique o elimine objetos de su bucket. Esto crea importantes riesgos de seguridad, incluida la posibilidad de que alguien suba archivos maliciosos, modifique los archivos existentes y elimine datos. El acceso de escritura pública crea vulnerabilidades de seguridad que pueden ser aprovechadas por los atacantes. Siguiendo los principios de seguridad estándar, AWS

recomienda restringir el acceso de escritura a sus buckets de Amazon S3 solo a los usuarios y sistemas necesarios.

1. Bloquee el acceso público a nivel de cuenta y de depósito

Amazon S3 proporciona ajustes de acceso público en bloque que se pueden configurar tanto a nivel de bucket como de cuenta para impedir el acceso público independientemente de las políticas del bucket o ACLs. Para obtener más información, consulte [Bloquear el acceso público a su almacenamiento de Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.

2. Modifique las políticas de bucket

Si desea utilizar un enfoque más detallado para eliminar el acceso público de escritura, revise la política de buckets. Puede buscar `s3:PutObject`, `s3:DeleteObject`, o `s3:*`. Para obtener más información sobre la administración de las políticas de [bucket](#), consulte [Políticas de bucket para Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.

3. Métodos de acceso alternativos Si se requiere un acceso de lectura público, considere estas alternativas más seguras:

- CloudFront— Úselo CloudFront con una identidad de acceso de origen (OAI) o un control de acceso de origen (OAC) para permitir el acceso de lectura desde un bucket privado de Amazon S3. Esta alternativa restringe el acceso directo a su bucket de Amazon S3 y, al mismo tiempo, permite que el contenido sea accesible públicamente a través CloudFront de él. Para obtener más información, consulte [Restringir el acceso a un origen de Amazon S3](#) en la Guía para CloudFront desarrolladores de Amazon.
- Prefirmado URLs: utilice prefirado URLs para acceder temporalmente a objetos específicos. Para obtener más información, consulte [Compartir objetos prefirados URLs](#) en la Guía del usuario de Amazon Simple Storage Service.

El punto de acceso Amazon S3 tiene habilitada la configuración de acceso público

Los puntos de acceso de Amazon S3 proporcionan un acceso personalizado a los conjuntos de datos compartidos en los buckets de Amazon S3. Al habilitar el acceso público a un punto de acceso, cualquier usuario de Internet podrá acceder a sus datos. Siguiendo los principios de seguridad estándar, AWS recomienda restringir el acceso público a los puntos de acceso de Amazon S3.

1. Cree un nuevo punto de acceso con el bloqueo de acceso público activado

Amazon S3 no admite cambiar la configuración de acceso público de un punto de acceso una vez creado un punto de acceso. Para obtener información sobre la creación de un punto de acceso, consulte [Administrar el acceso público a los puntos de acceso para buckets de uso general](#) en la Guía del usuario de Amazon S3. Para obtener más información sobre la administración del acceso público a los puntos de acceso, consulte [Creación de puntos de acceso para buckets de uso general](#) en la Guía del usuario de Amazon S3.

Características de los datos confidenciales de los buckets de Amazon S3

Estas son las características de los datos confidenciales de los buckets de Amazon S3 y las medidas de corrección sugeridas.

Características de los datos confidenciales de los buckets de Amazon S3

Cuando Macie identifica datos confidenciales en sus depósitos de Amazon S3, indica posibles riesgos de seguridad y conformidad que requieren atención inmediata.

Los datos confidenciales pueden incluir:

- Credenciales
- Información de identificación personal
- Información financiera
- Contenido confidencial que requiere protección

Si los datos confidenciales quedan expuestos debido a una mala configuración o a un acceso no autorizado, podrían producirse infracciones de conformidad, filtraciones de datos, robo de identidad o pérdidas económicas. Siguiendo las prácticas recomendadas de seguridad, AWS recomienda una clasificación adecuada de los datos y un monitoreo continuo de los datos confidenciales en sus buckets de Amazon S3.

Implemente controles para los datos confidenciales

En la búsqueda de exposición, elija el recurso Abierto. Revise el tipo de datos confidenciales detectados y su ubicación en el depósito. Para obtener ayuda para interpretar los hallazgos de Macie, consulte [Tipos de hallazgos de Macie en la Guía](#) del usuario de Amazon Macie.

En función del tipo de datos confidenciales descubiertos, implemente los controles de seguridad adecuados:

- Restrinja el acceso al depósito: revise los permisos del depósito para asegurarse de que siguen el principio del mínimo privilegio. Utilice las políticas de IAM y las políticas de bucket y restrinja el ACLs acceso. Para obtener más información, consulte [Identity and Access Management for Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.
- Habilite el cifrado del lado del servidor: habilite el cifrado del lado del servidor con claves y claves de KMS para una protección adicional. Para obtener más información, consulte [Uso del cifrado del lado del servidor con claves de AWS KMS \(SSE-KMS\) en la Guía del usuario](#) de Amazon Simple Storage Service.
- Uso AWS Glue DataBrew: utilícelo Glue DataBrew para la preparación y limpieza de datos. Para obtener más información, consulte [Contenido](#) de AWS Glue DataBrew la Guía para AWS Glue DataBrew desarrolladores.

Hallazgos de secuencias de ataques en Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Una [secuencia de ataque](#) es un tipo de amenaza a la seguridad. GuardDuty genera resultados para las secuencias de ataque cuando los eventos coinciden con un patrón de actividad sospechosa. Si lo [GuardDutyhabilitas](#), puedes acceder a este tipo de búsqueda en la consola de Security Hub. Esto le permite investigar y solucionar todas sus amenazas de seguridad sin tener que cambiar de consola. Puede revisar los resultados de la secuencia de ataques en la pantalla Amenazas de la consola de Security Hub.

Revisar los hallazgos de la secuencia de ataque

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Puede revisar los resultados de la secuencia de ataques en la pantalla Amenazas de la consola de Security Hub. En el siguiente tema se describe cómo revisar los detalles de una búsqueda de una secuencia de ataque.

Revisión de los detalles de los hallazgos de la secuencia de ataque

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

En este tema se describe cómo revisar los detalles sobre los hallazgos de la secuencia de ataques en la consola de Security Hub y con la API.

Revisión de los detalles de las secuencias de ataque en la consola de Security Hub

A continuación se describe cómo revisar los detalles de las secuencias de ataque en la consola de Security Hub:

Para revisar los resultados de la secuencia de ataques en la consola

1. ¿Inicia sesión con tus credenciales y abre la consola de Security Hub en la <https://console.aws.amazon.com/securityhub/v2/home? región=us-east-1>.
2. En el panel de navegación, seleccione Amenazas.
3. En la lista de resultados de la secuencia de ataque, elija el hallazgo de la secuencia de ataque del que desee ver los detalles.

Revisar los detalles de los hallazgos de la secuencia de ataque con la API

Puede revisar los hallazgos de la secuencia de ataque con la [GetFindingsV2](#) API o con AWS CLI. Puede filtrar los resultados con el [FindingProviderFields](#) parámetro y proporcionar un valor de filtro TTPs/AttackSequence si solo desea devolver los hallazgos de la secuencia de ataque. Puede filtrar por otros campos para acotar los resultados.

Comando de ejemplo:

A continuación se muestra un AWS CLI ejemplo en el que se recuperan los 10 hallazgos de secuencias de ataque generados más recientemente en su cuenta. El ejemplo está formateado para Linux, macOS y Unix, y el carácter de barra invertida (\) se utiliza para mejorar la legibilidad.

```
$ aws securityhub get-findings-v2 \
--filters '{"FindingProviderFieldsTypes":[{"Value": "TTPs/
AttackSequence", "Comparison": "PREFIX"}]}' \
```

```
--sort-criteria '{ "Field": "LastObservedAt", "SortOrder": "desc" }' \
--max-items 10
```

Corregir los hallazgos de la secuencia de ataques

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Para obtener información sobre cómo corregir los hallazgos de la secuencia de ataques, consulte [Remediar los hallazgos de GuardDuty seguridad detectados](#) en la Guía GuardDuty del usuario de Amazon.

Reglas de automatización en Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Las reglas de automatización de Security Hub son una versión más ampliable y configurable de las reglas de automatización [CSPM de Security Hub](#). Security Hub pasó de ser un sistema de automatización específico para la búsqueda a una plataforma de configuración más amplia. Mientras que el Security Hub CSPM es compatible con ASFF, Security Hub introduce el soporte para OCSF y sienta las bases para más configuraciones. Una de las características clave de las reglas de automatización de Security Hub es su integración con la configuración del agregador. Esto ofrece la posibilidad de ajustar e implementar las configuraciones de forma granular en un conjunto de dispositivos conectados, al Regiones de AWS tiempo que se mantiene la flexibilidad necesaria para configurar una experiencia regional y Regiones de AWS desvincularla una por una.

Los recursos de Security Hub que tengas en tu Cuenta de AWS Región de AWS mano, incluidas las reglas de automatización, los conectores y los agregadores, dejarán de funcionar en los siguientes escenarios.

- La persona independiente Cuenta de AWS pasa a ser miembro de una AWS organización con un administrador delegado

- La cuenta de administración de la AWS organización elimina al administrador delegado de la organización y establece un nuevo administrador delegado
- La configuración del agregador del administrador delegado o autónomo Cuenta de AWS se cambia para convertir una región desvinculada en una región vinculada

En estos escenarios, la cuenta del miembro aún puede administrar estos recursos únicamente mediante las operaciones de lista, obtención y eliminación. AWS CLI Cuando una región desvinculada se convierte en región vinculada, el administrador delegado o la AWS cuenta independiente pueden seguir gestionando los recursos antiguos de una región vinculada mediante las operaciones de lista, obtención y eliminación.

Mejoras clave

Las reglas de automatización de Security Hub CSPM son regionales y solo se aplican a los hallazgos en el Regiones de AWS lugar donde se crearon. Las reglas de automatización de Security Hub se pueden configurar una vez en una Región de AWS (región de agregación) y, a continuación, aplicarse en todas las regiones configuradas Regiones de AWS (regiones vinculadas) mediante la configuración Aggregator V2. Una de las ventajas de esta función es la capacidad de automatizar y corregir los hallazgos de seguridad en varios grupos con Regiones de AWS solo configurar uno. Región de AWS Esto significa que, si se genera un hallazgo en una región vinculada, se puede corregir automáticamente en función de la configuración de la región de agregación.

Integración externa

Las reglas de automatización de Security Hub admiten un tipo de acción para la creación de tickets de ITSM. Esto permite a los clientes dirigir los hallazgos seleccionados del OCSF directamente a una o más integraciones de ITSM configuradas. Si un hallazgo del OCSF coincide con los criterios, puede crear un ticket en o. Jira Cloud ServiceNow ITSM Para obtener más información, consulte [Integraciones de terceros para Security Hub](#).

Criterios compatibles con el OCSF

El CSPM de Security Hub admite la evaluación de los campos ASFF en función de los hallazgos, mientras que Security Hub hace coincidir los campos de OCSF. Por ejemplo, el conjunto de filtros compatibles con el Criteria parámetro utilizado en las reglas de automatización de la versión 2 coincide con el conjunto de filtros compatibles con el Criteria parámetro utilizado en. [GetFindingsV2](#) Esto significa que los filtros utilizados para recuperar los hallazgos de la V2 se pueden usar en una regla de automatización de la V2 que coincida con los hallazgos.

Campos OCSF para **AutomationRulesFindingFieldsUpdate**

La lista de campos que se pueden actualizar [AutomationRulesFindingFieldsUpdate](#) en Security Hub CSPM ha cambiado en Security Hub. Para [AutomationRulesFindingFieldsUpdateV2](#) la lista de campos que se pueden actualizar, incluya lo siguiente:

- Comment
- SeverityId
- StatusId

Integraciones de terceros para Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Puede mejorar su postura de seguridad con integraciones de terceros para AWS Security Hub. Con esta función, puede configurar su integración para crear incidentes o problemas para los hallazgos de Security Hub.

Cree una clave KMS para cifrar las credenciales

Los procedimientos de integración de esta sección le ofrecen la opción de cifrar sus credenciales con una AWS clave propia o gestionada por el cliente. Una clave AWS propia es una clave de KMS que no está en su poder Cuenta de AWS porque el AWS servicio que cifra sus credenciales es el propietario de la clave de KMS y la administra. Si quiere tener el control total de la clave KMS utilizada para cifrar sus credenciales, [cree una clave gestionada por el cliente](#). Una clave administrada por el cliente es una clave de KMS que usted posee y administra.

Acceso a las operaciones de cifrado de Security Hub

Esta declaración de política permite a Security Hub utilizar la AWS KMS clave para las operaciones de cifrado. Permite a Security Hub proteger los secretos de sus clientes con esta clave. Los permisos están restringidos a las operaciones relacionadas con conectores específicos de Security Hub a través del bloque de condiciones que comprueba el ARN de origen y el contexto de cifrado.

```
{
  "Sid": "Allow Security Hub access to the customer managed key",
  "Effect": "Allow",
  "Principal": {
    "Service": "connector.securityhub.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt",
    "kms:ReEncrypt*"
  ],
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:SourceArn": "arn:aws:securityhub:${Region}:${AccountId}:connectorv2/*"
    },
    "StringLike": {
      "kms:EncryptionContext:aws:securityhub:connectorV2Arn":
"arn:aws:securityhub:${Region}:${AccountId}:connectorv2/*",
      "kms:EncryptionContext:aws:securityhub:providerName":
"${CloudProviderName}"
    }
  }
}
```

Note

Para *CloudProviderName*, introduzca JIRA_CLOUD o. SERVICENOW Para *Region* y *AccountId*, introduzca su Cuenta de AWS ID Región de AWS y.

Acceso de lectura de claves a Security Hub

Esta declaración de política permite a Security Hub leer los metadatos sobre la clave KMS al permitir la DescribeKey operación. Este permiso es necesario para que Security Hub verifique el estado y la configuración de la clave. El acceso está limitado a conectores específicos de Security Hub a través de la condición de ARN de origen.

```
{
  "Sid": "Allow Security Hub read access to the customer managed key",
  "Effect": "Allow",
```

```

    "Principal": {
      "Service": "connector.securityhub.amazonaws.com"
    },
    "Action": [
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:securityhub:${Region}:${AccountId}:connectorv2/*"
      }
    }
  }
}

```

Note

Para *Region* y *AccountId*, introduzca su Cuenta de AWS ID Región de AWS y.

Acceso principal de IAM para las operaciones del Security Hub

[Esta declaración de política otorga al rol de IAM especificado permisos para realizar operaciones clave \(describir, generar, descifrar, volver a cifrar y enumerar los alias\) al interactuar con Security Hub mediante la V2 y la V2. CreateConnector CreateTicket APIs](#) La condición garantiza que estas operaciones solo se puedan realizar a través del servicio Security Hub en la región especificada.

```

{
  "Sid": "Allow permissions to access key through Security Hub",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::${AccountId}:role/${RoleName}"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt",
    "kms:ReEncrypt*"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": [
        "securityhub.${Region}.amazonaws.com"
      ]
    }
  }
}

```

```

        ]
      },
      StringLike: {
        "kms:EncryptionContext:aws:securityhub:providerName": "SERVICENOW"
      }
    }
  }

{
  "Sid": "Allow read permissions to access key through Security Hub",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::${AccountId}:role/${RoleName}"
  },
  "Action": [
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": [
        "securityhub.${Region}.amazonaws.com"
      ]
    }
  }
}

```

Note

Para *RoleName*, introduzca el nombre del rol de IAM que realiza las llamadas a Security Hub. Para *Region* y *AccountId*, introduzca su Cuenta de AWS ID Región de AWS y.

Integraciones para AWS Security Hub Jira Cloud

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

En este tema se describe cómo acceder a la consola de Security Hub para configurar una integración Jira Cloud. Antes de completar cualquiera de los procedimientos de este tema, debe adquirir un plan de Jira Cloud suscripción. Para obtener información sobre los planes de suscripción, consulte [los precios](#) en el Atlassian sitio web.

Requisitos previos

Complete los siguientes requisitos previos antes de configurar una integración para Jira Cloud.

1. Instale Security Hub para Jira Cloud

El siguiente procedimiento describe cómo instalar el complemento necesario.

1. Inicie sesión en su Atlassian sitio como administrador.
2. Ve a la configuración del sitio y selecciona Descubrir nuevas aplicaciones.
3. Seleccione Security Hub para Jira Cloud y elija Obtener aplicación.

2. Crea un proyecto (si aún no lo has creado)

Este paso es obligatorio si no has creado un proyecto. Para obtener información sobre cómo crear un proyecto, consulte [Crear un proyecto nuevo](#) en la Jira Cloud Support documentación.

Requisitos para crear un proyecto

Asegúrese de hacer lo siguiente al crear un nuevo proyecto.

- Elija Desarrollo de software para la plantilla del proyecto.
- Elija Gestionado por la empresa para el tipo de proyecto.
- Anote la clave del proyecto.

3. Añada sus proyectos de desarrollo de software al Security Hub para Jira Cloud aplicaciones

El siguiente procedimiento describe cómo añadir sus proyectos de desarrollo de software al Security Hub para Jira Cloud aplicaciones.

1. Inicie sesión en su Atlassian sitio como administrador.
2. Ve a la configuración del sitio y selecciona Descubrir nuevas aplicaciones.
3. En el panel de navegación, en Aplicaciones, elija Security Hub CSPM V2.
4. Seleccione la pestaña de configuración del conector.

5. En Proyectos activados, selecciona Añadir proyecto de Jira.
 - a. En el menú desplegable, selecciona Añadir todo o selecciona un proyecto. Repite esta parte del paso si quieres añadir más de un proyecto, pero no todos los proyectos.
 - b. Seleccione Save.

 Note

Puede seleccionar la pestaña Gestor de instalación para comprobar que todos los proyectos que ha seleccionado se han instalado correctamente.

Para obtener información adicional al respecto Jira Cloud, consulte [Jira Cloud los recursos](#) del sitio Atlassian web.

Recomendaciones

Las siguientes son recomendaciones que se deben tener en cuenta antes de configurar una integración para Jira Cloud.

- Cree una cuenta de sistema dedicada en Jira Cloud.
- Utilice una cuenta de sistema por Jira Cloud instancia.

Configure una integración para Jira Cloud

Security Hub crea problemas automáticamente en Jira Cloud. Esta integración le permite enviar las conclusiones del Security Hub a Jira Cloud, para que pueda gestionarlos como parte de sus flujos de trabajo operativos. Por ejemplo, puede asignar la propiedad a los problemas que deban investigarse y solucionarse. Debe completar el siguiente procedimiento para cada uno de los Jira Cloud proyectos a los que desee enviar las conclusiones de Security Hub.

 Note

Al crear un Jira Cloud conector, se le redirige del conector actual Región de AWS a para "https://3rdp.oauth.console.api.aws" que pueda completar el registro del conector. Después, volverá al Región de AWS lugar donde se está creando el conector.

Para configurar una integración para Jira Cloud

1. ¿Inicia sesión en tu AWS cuenta con tus credenciales y abre la consola de Security Hub en la <https://console.aws.amazon.com/securityhub/versión 2/home? región=us-east-1>.
2. En el panel de navegación, elija Administración y, a continuación, Integraciones.
3. Elija Agregar Jira Cloud.
4. Para obtener más información, introduzca un nombre único y descriptivo para la integración y determine si desea introducir una descripción opcional para la integración.
5. En cuanto a la configuración de seguridad, decide cómo cifrar tus Jira Cloud credenciales en Security Hub. Si elige la clave propiedad del servicio, se utilizará una AWS clave propia para cifrar sus datos. Si elige Clave personalizada, debe introducir el ARN de una clave personalizada existente o crear una clave nueva seleccionando Crear una AWS KMS clave. Para obtener información sobre cómo crear una clave KMS, consulte [Crear una clave KMS de cifrado simétrico](#).

Note

No puede cambiar esta configuración una vez que haya completado esta configuración. Sin embargo, si elige la clave personalizada, puede editar la política de claves personalizadas en cualquier momento.

6. (Opcional) Para las etiquetas, cree y añada una etiqueta a su integración. Puede añadir hasta 50 etiquetas.
7. Para las autorizaciones, elija Crear conector y autorizar. Aparece una ventana emergente en la que selecciona Permitir para completar la autorización. Después de completar la autorización, aparece una casilla de verificación que le indica que la autorización se ha realizado correctamente.
8. En el caso de las configuraciones, introduzca el ID Jira Cloud del proyecto.
9. Elija Configuración completa. Tras completar la configuración, puede ver las integraciones configuradas en la pestaña Integraciones configuradas.

Crear un ticket para una integración Jira Cloud

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Después de crear una integración con Jira Cloud, puede crear un ticket para un hallazgo.

Note

Un hallazgo siempre estará asociado a un único ticket durante todo su ciclo de vida. Todas las actualizaciones posteriores de un hallazgo tras su creación inicial se enviarán al mismo ticket. Si se cambia un conector asociado a una regla de automatización, el conector actualizado solo se utilizará para los hallazgos nuevos y entrantes que coincidan con los criterios de la regla.

Para crear un ticket para un hallazgo

1. ¿Inicia sesión en tu AWS cuenta con tus credenciales y abre la consola de Security Hub en la <https://console.aws.amazon.com/securityhub/version-2/home? región=us-east-1>.
2. En el panel de navegación, en Inventario, selecciona Hallazgos.
3. Elige un hallazgo. En la búsqueda, selecciona Crear ticket.
4. Para la integración, abre el menú desplegable y selecciona una integración. Esta integración es la que creaste anteriormente al configurar el Jira Cloud proyecto. Elija la integración a la que desea que se envíen los resultados.
5. Seleccione Crear.

Visualización de un ticket para una Jira Cloud integración

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Después de crear un ticket para un hallazgo, puedes abrir el ticket en tu Jira Cloud instancia.

Para ver un hallazgo en su Jira Cloud instancia

1. ¿Inicia sesión en tu AWS cuenta con tus credenciales y abre la consola de Security Hub en la <https://console.aws.amazon.com/securityhub/versión 2/home? región=us-east-1>.
2. En el panel de navegación, en Inventario, selecciona Hallazgos.
3. Elija el hallazgo en el que creó el ticket.
4. En la búsqueda, elige el ID del ticket para ver el ticket en tu Jira Cloud instancia o Ver JSON.

Integraciones para ServiceNow

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

En este tema se describe cómo acceder a la consola de Security Hub para configurar una integración ServiceNow ITSM. Antes de completar cualquiera de los procedimientos de este tema, debe tener una suscripción para ServiceNow ITSM poder agregar esta integración. Para obtener más información, consulte [la página de precios](#) del sitio ServiceNow web.

Requisitos previos

Complete los siguientes requisitos previos antes de configurar una integración para ServiceNow ITSM.

1. Instalar Security Hub V2 encuentra la integración para la gestión de servicios de TI (ITSM)

El siguiente procedimiento describe cómo instalar el complemento Security Hub V2.

1. Inicie sesión en la ServiceNow ITSM instancia y, a continuación, abra el navegador de aplicaciones.
2. Ve a la [ServiceNow tienda](#).
3. Busque Security Hub V2, busque la integración para la administración de servicios de TI (ITSM) y, a continuación, elija Obtener para instalar la aplicación.

 Note

En la configuración de la aplicación Security Hub V2, elija qué acción desea realizar cuando se envíen nuevos hallazgos del Security Hub a su ServiceNow ITSM entorno. Puede elegir No hacer nada, Crear incidente, Crear problema o Crear ambas opciones (incidente/problema)

2. Configure el tipo de concesión de credenciales de cliente para las solicitudes entrantes OAuth

Debe configurar este tipo de concesión para las solicitudes entrantes OAuth . Para obtener más información, consulte El [tipo de concesión de credenciales de cliente para Inbound OAuth se admite](#) en la página web ServiceNow Support.

3. Crea una aplicación OAuth

Si ya ha creado una OAuth aplicación, puede omitir este requisito previo. Para obtener información sobre la creación de una OAuth aplicación, consulte [Configuración OAuth](#).

Configure una integración para ServiceNow ITSM

Security Hub puede crear incidentes o problemas automáticamente enServiceNow ITSM.

Para configurar una integración para ServiceNow ITSM

1. ¿Inicia sesión en tu AWS cuenta con tus credenciales y abre la consola de Security Hub en la <https://console.aws.amazon.com/securityhub/versión 2/home? región=us-east-1>.
2. En el panel de navegación, elija Administración y, a continuación, Integraciones.
3. En ServiceNow ITSM, selecciona Añadir integración.
4. Para obtener más información, introduzca un nombre para la integración y determine si desea introducir una descripción opcional para la integración.
5. En cuanto a la configuración de seguridad, decide cómo cifrar tus Jira Cloud credenciales en Security Hub. Si elige la clave propiedad del servicio, se utilizará una AWS clave propia para cifrar sus datos. Si elige Clave personalizada, debe introducir el ARN de una clave personalizada existente o crear una clave nueva seleccionando Crear una AWS KMS clave. Para obtener información sobre cómo crear una clave KMS, consulte [Crear una clave KMS de cifrado simétrico](#).

Note

No puede cambiar esta configuración una vez que haya completado esta configuración. Sin embargo, si elige la clave personalizada, puede editar la política de claves personalizadas en cualquier momento.

6. Para las autorizaciones, introduce ServiceNow ITSM la URL, el ID de cliente y el secreto del cliente.
7. En el caso de las etiquetas, determine si desea crear y añadir una etiqueta opcional a la integración.
8. Elija Configuración completa. Tras completar la configuración, puede ver las integraciones configuradas en la pestaña Integraciones configuradas.

Crear un ticket para una integración ServiceNow ITSM

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Después de crear una integración con ServiceNow ITSM, puede crear un ticket para un hallazgo.

Note

Un hallazgo siempre estará asociado a un único ticket durante todo su ciclo de vida. Todas las actualizaciones posteriores de un hallazgo tras su creación inicial se enviarán al mismo ticket. Si se cambia un conector asociado a una regla de automatización, el conector actualizado solo se utilizará para los hallazgos nuevos y entrantes que coincidan con los criterios de la regla.

Para crear un ticket para un hallazgo

1. ¿Inicia sesión en tu AWS cuenta con tus credenciales y abre la consola de Security Hub en la <https://console.aws.amazon.com/securityhub/versión 2/home? región=us-east-1>.
2. En el panel de navegación, en Inventario, selecciona Hallazgos.

3. Elige un hallazgo. En la búsqueda, selecciona Crear ticket.
4. Para la integración, abre el menú desplegable y selecciona una integración.
5. Seleccione Crear.

Ver un ticket para una integración ServiceNow ITSM

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Después de crear un ticket para un hallazgo, puedes abrir el ticket en tu ServiceNow ITSM instancia.

Para ver un hallazgo en su ServiceNow ITSM instancia

1. ¿Inicia sesión en tu AWS cuenta con tus credenciales y abre la consola de Security Hub en la <https://console.aws.amazon.com/securityhub/versión 2/home? región=us-east-1>.
2. En el panel de navegación, en Inventario, selecciona Hallazgos.
3. Elija el hallazgo en el que creó el ticket.
4. En la búsqueda, elige el ID del ticket para ver el ticket en tu ServiceNow ITSM instancia o Ver JSON.

Trabajar en el panel de resumen de Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

En este tema se describe el panel de resumen de la consola de Security Hub. En esta página se muestra un resumen de las exposiciones, las amenazas, los principales recursos y la cobertura de los servicios de seguridad en varios widgets de seguridad. Estos widgets le ayudan a visualizar las exposiciones y las amenazas por gravedad y por capacidad de seguridad. Cada vez que abre esta página, los datos se actualizan automáticamente.

Puede personalizar esta página añadiendo y quitando distintos widgets de seguridad y estableciendo criterios de filtrado para recuperar datos específicos de cada widget. Las personalizaciones de esta página se guardan para usarlas en el futuro. Si su cuenta es la cuenta de administrador delegado de una organización, las personalizaciones se guardan independientemente de las personalizaciones de las cuentas de los miembros.

Note

Le recomendamos que no incluya información confidencial, confidencial o de identificación personal (PII) en los filtros guardados, los widgets personalizados u otros campos de texto de formato libre relacionados.

Si tu cuenta es la cuenta de administrador delegado de una organización, los datos incluyen los resultados de tu cuenta y de las cuentas de los miembros. Si su cuenta es una cuenta de miembro o una cuenta independiente, los datos solo incluyen los hallazgos de su cuenta. Si configura la agregación entre regiones en Security Hub, en esta página se muestran los resultados de la agregación.

El widget de resumen de exposiciones

Este widget muestra todas las exposiciones por gravedad. Puede ver la frecuencia de cada exposición en su entorno. Las exposiciones con mayor gravedad aparecen primero. Las exposiciones se basan en un análisis de los hallazgos y características de Security Hub y otros Servicios de AWS, como Amazon Inspector. La lista de exposiciones de este widget se limita a las ocho exposiciones más altas con el mayor número de hallazgos críticos. Si dos o más exposiciones tienen el mismo número de hallazgos críticos, la lista agrupa automáticamente esos hallazgos detrás de los hallazgos críticos más recientes.

El widget de resumen de amenazas

Este widget muestra todas las amenazas por gravedad. Las amenazas con mayor gravedad aparecen primero. Las amenazas están relacionadas con una serie de eventos e identifican las posibles amenazas en su entorno. También se originan en GuardDuty. La lista de amenazas de este widget se limita a las ocho amenazas de mayor gravedad. Si dos o más amenazas son de la misma gravedad, la lista agrupa automáticamente esas conclusiones en función de las más recientes. Debe habilitar GuardDuty la recepción de datos en este widget.

El widget de cobertura de seguridad

Este widget muestra un resumen de tu cobertura de seguridad y se basa en los resultados de cobertura de los servicios compatibles. Muestra las comprobaciones de cobertura que se han aprobado, las que han fallado o las que no están disponibles. Si no está disponible, indica que no se pudo completar la verificación de cobertura. Esto puede deberse a la eliminación de un recurso o a un fallo del servidor.

Los porcentajes de las comprobaciones de cobertura se refieren al número de comprobaciones que se aprobaron y no se aprobaron. Por ejemplo, se aprueba una verificación de cobertura y otra no. Esto indica que se han aprobado el 50% de sus controles y que el 50% de ellos han sido rechazados. En algunos casos, los porcentajes se redondean al número entero más cercano.

A diferencia de los servicios de seguridad como GuardDuty Amazon Inspector y Macie, Security Hub CSPM publica un dato de cobertura por cuenta, que PASS/FAIL depende de los estándares habilitados, como PASS si hay al menos un estándar habilitado. Los porcentajes de cobertura de Security Hub CSPM son el número de hallazgos de cobertura de CSPM de Security Hub que pasaron al número total de hallazgos de cobertura de CSPM de Security Hub.

Note

Le recomendamos que no incluya información confidencial, sensible o de identificación personal (PII) en los filtros guardados, los widgets personalizados u otros campos de texto de formato libre relacionados.

Visualización de detalles sobre los recursos en Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

La página de recursos hace un seguimiento de los recursos comunes de tu cuenta. Para acceder a la página Recursos de la consola de Security Hub, seleccione Recursos en el panel de navegación. Al elegir un tipo de recurso, puede revisar todos los recursos asociados al tipo de recurso. Puede revisar cualquier hallazgo asociado a un recurso.

 Note

El administrador delegado puede ver todos los recursos asociados a las cuentas de los miembros. Si configuraste un hogar Región de AWS, puedes ver todos los recursos de tu hogar Región de AWS desde Linked Regiones de AWS.

Si eliges un recurso, puedes revisar los detalles de ese recurso. Estos detalles incluyen el nombre, el ID, el ARN, el tipo y la categoría del recurso. Puede revisar el ID de cuenta asociado al recurso, cuándo se creó el recurso (marca de tiempo) y dónde se creó el recurso (). Región de AWS También puedes revisar los detalles adicionales en un fragmento de código JSON que puedes copiar.

Si cambias de la pestaña Descripción general a la pestaña Hallazgos, puedes revisar cualquier hallazgo asociado al recurso. La pestaña Hallazgos muestra el nombre de cada hallazgo, el tipo y la gravedad de cada hallazgo. Puede agrupar los hallazgos por diferentes campos y buscarlos mediante filtros. Si eliges un hallazgo, puedes revisar una descripción general del hallazgo, que incluye información sobre el cumplimiento y cómo solucionar los problemas asociados con el hallazgo. Si vuelve al recurso, puede elegir Abrir recurso para revisar el tipo de recurso correspondiente al recurso en la consola. Por ejemplo, si el recurso es un recurso de IAM, puede abrirlo en la consola de IAM.

La página de recursos le proporciona diferentes formas de organizar y buscar recursos. Puede agrupar los recursos por tipo. Por ejemplo, puede agrupar los recursos por identificador de cuenta, tipo de búsqueda Región de AWS, categoría de recurso, nombre y tipo de recurso. Puede buscar los resultados mediante filtros. Los filtros rápidos le ayudan a revisar los recursos por categoría, cuentas y tipos de búsqueda.

La ventaja de la página de recursos es que le ayuda a supervisar su nivel de seguridad, organizar los recursos y revisar los detalles de los mismos.

Visualización de las exposiciones en Security Hub con el gráfico de posibles rutas de ataque

 Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

El gráfico de la posible trayectoria de un ataque es una visualización interactiva que muestra cómo los posibles atacantes pueden acceder a los recursos asociados a una detección de exposición y hacerse con el control de ellos. Puede acceder a este gráfico solo en la consola de Security Hub y desde la pantalla Exposiciones. Al ver los detalles de un hallazgo de exposición, la pestaña Descripción general incluye una sección llamada Posible ruta de ataque.

En esta sección de la pestaña Descripción general, puedes seleccionar y arrastrar AWS los recursos al gráfico de la posible ruta de ataque. Puedes centrarte en áreas específicas del gráfico de la ruta de ataque con los iconos de zoom para acercar y alejar la imagen. Puedes ampliar el gráfico de la ruta de ataque dentro y fuera del modo de pantalla completa mediante el icono de pantalla completa. La leyenda codifica el recurso principal, el recurso implicado y el recuento de rasgos contribuyentes por color, y muestra las categorías de rasgos y el número de rasgos en el gráfico de la ruta de ataque. Para ver los detalles de un recurso, selecciona un recurso y selecciona Ver detalles del recurso. También puede copiar el identificador y el Cuenta de AWS número asociados a un recurso. Los hallazgos de exposición con un rasgo de accesibilidad muestran la conexión pública a Internet y la red colapsada en el gráfico de la ruta de ataque. Para ver este detalle, seleccione el nodo de la ruta de red colapsada.

Deshabilitación de Security Hub

Note

Security Hub se encuentra en versión preliminar y está sujeto a cambios.

Si tu cuenta no forma parte de una organización, puedes deshabilitar Security Hub en la consola del Security Hub en cualquier momento. Al deshabilitar Security Hub, deja de ingerir los hallazgos. También pierde el acceso a los hallazgos y configuraciones existentes. El siguiente procedimiento describe cómo deshabilitar Security Hub.

Para deshabilitar Security Hub

1. Inicie sesión en su AWS cuenta con sus credenciales y abra la consola de Security Hub en la <https://console.aws.amazon.com/securityhub/versión 2/home>.
2. En el panel de navegación, selecciona General.
3. En Security Hub, selecciona Desactivar. En la ventana emergente, escribe Desactivar y selecciona Desactivar.

¿Qué es AWS Security Hub CSPM?

AWS Security Hub Cloud Security Posture Management (CSPM) le proporciona una visión completa del estado de su seguridad y le ayuda a evaluar su AWS entorno según los estándares AWS y las mejores prácticas del sector de la seguridad.

Security Hub CSPM recopila datos de seguridad de todos Cuentas de AWS los productos de terceros compatibles y los ayuda a analizar las tendencias de seguridad e identificar los problemas de seguridad más prioritarios. Servicios de AWS

Para ayudarle a gestionar el estado de seguridad de su organización, Security Hub CSPM admite varios estándares de seguridad. Estos incluyen el estándar de mejores prácticas de seguridad AWS fundamentales (FSBP) desarrollado por AWS, y marcos de cumplimiento externos, como el Centro de Seguridad de Internet (CIS), el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) y el Instituto Nacional de Estándares y Tecnología (NIST). Cada estándar incluye varios controles de seguridad, cada uno de los cuales representa una práctica de seguridad recomendada. Security Hub CSPM comprueba los controles de seguridad y genera resultados de control para ayudarle a evaluar su conformidad con las mejores prácticas de seguridad.

Además de generar resultados de control, Security Hub CSPM también recibe hallazgos de otros productos Servicios de AWS(como Amazon, Amazon GuardDuty Inspector y Amazon Macie) y de productos de terceros compatibles. De este modo, podrá ver varios problemas relacionados con la seguridad en un único panel. También puede enviar las conclusiones del CSPM de Security Hub a otros productos Servicios de AWS de terceros compatibles.

Security Hub CSPM ofrece funciones de automatización que le ayudan a clasificar y solucionar los problemas de seguridad. Por ejemplo, puede usar reglas de automatización para actualizar automáticamente resultados críticos cuando un control de seguridad falla. También puedes aprovechar la integración con Amazon EventBridge para activar respuestas automáticas a hallazgos específicos.

Temas

- [Ventajas de Security Hub CSPM](#)
- [Acceso a Security Hub \(CSPM\)](#)
- [Servicios relacionados](#)
- [Precio y prueba gratuitos de Security Hub CSPM](#)

Ventajas de Security Hub CSPM

Estas son algunas de las formas clave en las que Security Hub CSPM le ayuda a supervisar el cumplimiento y la postura de seguridad en todo su AWS entorno.

Reducción del esfuerzo para recopilar y priorizar los resultados

Security Hub CSPM reduce el esfuerzo de recopilar y priorizar los hallazgos de seguridad en las cuentas de los productos integrados Servicios de AWS y de AWS socios. Security Hub CSPM procesa la búsqueda de datos mediante el AWS Security Finding Format (ASFF), un formato de búsqueda estándar. Esto elimina la necesidad de administrar los resultados de numerosas fuentes en varios formatos. Security Hub CSPM también correlaciona los hallazgos entre los proveedores para ayudarlo a priorizar los más importantes.

Controles de seguridad automáticos respecto a las prácticas recomendadas y a los estándares

Security Hub CSPM ejecuta automáticamente comprobaciones continuas de configuración y seguridad a nivel de cuenta según las AWS mejores prácticas y los estándares del sector. Security Hub CSPM utiliza los resultados de estas comprobaciones para calcular las puntuaciones de seguridad e identifica cuentas y recursos específicos que requieren atención.

Vista consolidada de los resultados en cuentas y proveedores

Security Hub CSPM consolida sus hallazgos de seguridad en todas las cuentas y los productos de los proveedores y muestra los resultados en la consola CSPM de Security Hub. También puede recuperar los resultados a través de la API CSPM de Security Hub AWS CLI, o. SDKs. Con una visión integral del estado actual de su seguridad, puede detectar tendencias, identificar posibles problemas y tomar las medidas de corrección necesarias.

Capacidad para automatizar la actualización y corrección de resultados

Puede crear reglas de automatización que modifiquen o supriman resultados en función de los criterios que haya definido. Security Hub CSPM también admite una integración con Amazon EventBridge. Para automatizar la corrección de resultados específicos, puede definir acciones personalizadas que se deben llevar a cabo cuando se genera un resultado. Por ejemplo, puede configurar acciones personalizadas para enviar resultados a un sistema de tickets o a un sistema de corrección automático.

Acceso a Security Hub (CSPM)

Security Hub CSPM está disponible en la mayoría. Regiones de AWS Para obtener una lista de las regiones en las que el CSPM de Security Hub está disponible actualmente, consulte los [puntos finales y las cuotas de AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) en el. Referencia general de AWS Para obtener más información sobre la administración Regiones de AWS para usted Cuenta de AWS, consulte [Especificar qué Regiones de AWS cuenta puede usar](#) en la Guía de referencia.AWS Account Management

En cada región, puede acceder y utilizar Security Hub CSPM de cualquiera de las siguientes maneras:

Consola Security Hub CSPM

AWS Management Console Es una interfaz basada en un navegador que puede usar para crear y administrar recursos. AWS Como parte de esa consola, la consola CSPM de Security Hub proporciona acceso a la cuenta, los datos y los recursos de Security Hub CSPM. Puede realizar tareas de CSPM de Security Hub mediante la consola de CSPM de Security Hub: ver los resultados, crear reglas de automatización, crear una región de agregación y mucho más.

API CSPM de Security Hub

La API CSPM de Security Hub le proporciona acceso programático a su cuenta, datos y recursos de Security Hub CSPM. Con la API, puede enviar solicitudes HTTPS directamente a Security Hub CSPM. Para obtener información sobre la API, consulta la referencia de la [API AWS Security Posture Management \(CSPM\) de Security Hub Cloud](#).

AWS CLI

Con el AWS CLI, puede ejecutar comandos en la línea de comandos de su sistema para realizar tareas de CSPM de Security Hub. En algunos casos, el uso de la línea de comandos puede ser más rápido y cómodo que usar la consola. La línea de comandos también es útil si desea crear scripts que realicen tareas. Para obtener información sobre la instalación y el uso del AWS CLI, consulte la Guía del [AWS Command Line Interface usuario](#).

AWS SDKs

AWS proporciona información SDKs que consta de bibliotecas y código de muestra para varios lenguajes de programación y plataformas, por ejemplo, Java, Go, Python, C++ y .NET. SDKs Proporcionan un acceso cómodo y programático a Security Hub, CSPM y otros Servicios de AWS en el idioma que prefiera. También permiten realizar tareas como firmar solicitudes

criptográficamente, administrar errores y reintentar solicitudes automáticamente. Para obtener información sobre la instalación y el uso de AWS SDKs, consulte [Herramientas sobre las que basarse](#). AWS

 Important

Security Hub CSPM solo detecta y consolida los hallazgos que se generan después de habilitar Security Hub CSPM. No detecta ni consolida retroactivamente los hallazgos de seguridad que se generaron antes de activar Security Hub CSPM.

Security Hub CSPM solo recibe y procesa los hallazgos en la región en la que habilitaste Security Hub CSPM en tu cuenta.

Para cumplir plenamente con las comprobaciones de seguridad de CIS AWS Foundations Benchmark, debe habilitar Security Hub CSPM en todas las regiones compatibles AWS .

Servicios relacionados

Para proteger aún más su AWS entorno, considere la posibilidad de utilizar otros Servicios de AWS en combinación con Security Hub CSPM. Algunos Servicios de AWS envían sus hallazgos al Security Hub CSPM, y Security Hub CSPM normaliza los hallazgos en un formato estándar. Algunos también Servicios de AWS pueden recibir las conclusiones del Security Hub CSPM.

Para obtener una lista de otros Servicios de AWS que envían o reciben las conclusiones del CSPM de Security Hub, consulte. [Servicio de AWS integraciones con Security Hub CSPM](#)

Security Hub CSPM utiliza reglas vinculadas a servicios AWS Config para ejecutar las comprobaciones de seguridad de la mayoría de los controles. Los controles se refieren a recursos específicos. Servicios de AWS Para obtener una lista de los controles CSPM de Security Hub, consulte. [Referencia de control para Security Hub CSPM](#) Debe habilitar AWS Config y registrar los recursos AWS Config para que Security Hub CSPM genere la mayoría de las conclusiones de control. Para obtener más información, consulte [Consideraciones antes de habilitar y configurar AWS Config](#).

Precio y prueba gratuitos de Security Hub CSPM

Al activar Security Hub CSPM en un Cuenta de AWS por primera vez, esa cuenta se inscribe automáticamente en una prueba gratuita de 30 días de Security Hub CSPM.

Cuando utilice Security Hub CSPM durante la prueba gratuita, se le cobrará por el uso de otros servicios con los que interactúa Security Hub CSPM, como los artículos. AWS Config No se le cobrará por AWS Config las reglas que se activen únicamente según los estándares de seguridad CSPM de Security Hub.

No se le cobrará por usar Security Hub CSPM hasta que finalice la prueba gratuita.

Visualización de detalles de uso y costo estimado

Security Hub CSPM proporciona información de uso, incluido un costo estimado de 30 días por usar Security Hub CSPM. Los detalles de uso incluyen el tiempo restante de la prueba gratuita. La información de uso puede ayudarle a comprender cuáles pueden ser los costes del CSPM de Security Hub una vez finalice la prueba gratuita. La información de uso también está disponible una vez finalizada la prueba gratuita.

Cómo mostrar la información de uso (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Uso en Configuración.

El coste mensual estimado se basa en el uso del Security Hub (CSPM) de tu cuenta para las comprobaciones y comprobaciones de seguridad previstas para un período de 30 días.

La información de uso y el costo estimado solo afectan a la cuenta y la región actuales. En una región de agregación, la información de uso y el costo estimado no incluyen las regiones vinculadas. Para obtener más información acerca de las regiones vinculadas, consulte [the section called “Tipos de datos que se agregan”](#).

Información sobre precios

Para obtener más información sobre cómo cobra Security Hub CSPM por los hallazgos ingeridos y las comprobaciones de seguridad, consulte los precios de CSPM [de Security Hub](#).

Conceptos y terminología en Security Hub CSPM

En AWS Security Hub Cloud Security Posture Management (CSPM), nos basamos en AWS conceptos y terminología comunes y utilizamos estos términos adicionales.

Cuenta

Una cuenta estándar de Amazon Web Services (AWS) que contiene tus AWS recursos. Puedes iniciar sesión AWS con tu cuenta y activar Security Hub CSPM.

Una cuenta puede invitar a otras cuentas a activar Security Hub CSPM y asociarse a esa cuenta en Security Hub CSPM. La aceptación de una invitación de suscripción es opcional. Si las invitaciones se aceptan, la cuenta se convierte en la cuenta de administrador, mientras que las cuentas añadidas se convierten en cuentas miembro. Las cuentas de administrador pueden ver los resultados de sus cuentas miembro.

Si está inscrito AWS Organizations, su organización designa una cuenta de administrador CSPM de Security Hub para la organización. La cuenta de administrador CSPM de Security Hub puede habilitar otras cuentas de la organización como cuentas de miembros.

Una cuenta no puede ser cuenta de administrador y cuenta miembro al mismo tiempo. Una cuenta solo puede tener una cuenta de administrador.

Para obtener más información, consulte [Administrar las cuentas de administrador y miembro en Security Hub \(CSPM\)](#).

Cuenta de administrador

Una cuenta de Security Hub CSPM a la que se le concede acceso para ver los resultados de las cuentas de los miembros asociadas.

Una cuenta se convierte en cuenta de administrador de las siguientes formas:

- La cuenta invita a otras cuentas a asociarse a ella en Security Hub CSPM. Cuando esas cuentas aceptan la invitación, pasan a ser cuentas miembro y la cuenta que las ha invitado se convierte en su cuenta de administrador.
- Una cuenta de administración de la organización designa la cuenta como cuenta de administrador CSPM de Security Hub. La cuenta de administrador CSPM de Security Hub puede habilitar cualquier cuenta de la organización como cuenta de miembro y también puede invitar a otras cuentas a ser cuentas de miembro.

Una cuenta solo puede tener una cuenta de administrador. Una cuenta no puede ser cuenta de administrador y cuenta miembro al mismo tiempo.

Región de agregación

La configuración de una región de agregación le permite ver los hallazgos de seguridad desde varios puntos de vista Regiones de AWS en un solo panel.

La región de agregación es la región desde la que se visualizan y administran los resultados. Los resultados se agregan a la región de agregación desde las regiones vinculadas. Las actualizaciones de los resultados se reproducen en todas las regiones.

En la región de agregación, las páginas de Estándares de seguridad, Información y Resultados contienen datos de todas las regiones vinculadas.

Para obtener más información, consulte [Agregación de datos del CSPM en todas las regiones](#).

Resultado archivado

Un hallazgo cuyo estado de registro es (RecordState)ARCHIVED. Archivar un resultado indica que el proveedor del mismo cree que dicho resultado ya no es relevante. El estado del registro es diferente del estado del flujo de trabajo, que rastrea el estado de la investigación de un hallazgo.

Los proveedores de búsqueda pueden utilizar el [BatchImportFindings](#) funcionamiento de la API CSPM de Security Hub para archivar los hallazgos que hayan creado. Security Hub CSPM archiva automáticamente los hallazgos de control que cumplen ciertos criterios. Para obtener más información, consulte [Generar, actualizar y archivar las conclusiones de control](#).

En la consola CSPM de Security Hub, la configuración de filtro predeterminada excluye las conclusiones archivadas de las listas y tablas de búsqueda. Puede actualizar la configuración para incluir las conclusiones archivadas. Si recupera las conclusiones mediante la [GetFindings](#) operación de la API CSPM de Security Hub, la operación recupera las conclusiones archivadas y activas. Para excluir las conclusiones archivadas, puede filtrarlas. Por ejemplo:

```
"RecordState": [  
  {  
    "Comparison": "EQUALS",  
    "Value": "ARCHIVED"  
  }  
],
```


AWS Formato de búsqueda de seguridad (ASFF)

Formato estandarizado para el contenido de las conclusiones que Security Hub CSPM agrega o genera. El formato AWS Security Finding le permite utilizar Security Hub CSPM para ver y analizar los hallazgos generados por los servicios de seguridad, las soluciones de terceros o el propio AWS Security Hub CSPM a partir de la ejecución de comprobaciones de seguridad. Para obtener más información, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

Controlar

Una salvaguardia o contramedida prescrita para un sistema de información o una organización diseñada para proteger la confidencialidad, integridad y disponibilidad de su información y para cumplir un conjunto de requisitos de seguridad definidos. Un estándar de seguridad está asociado a un conjunto de controles.

El término control de seguridad se refiere a los controles que tienen un ID y un título de control únicos en todos los estándares. El término control estándar se refiere a los controles que tienen controles y títulos específicos de un estándar. IDs Actualmente, Security Hub CSPM admite controles estándar solo en las regiones de China y. AWS GovCloud (US) Regions Los controles de seguridad son compatibles en todas las demás regiones.

Acción personalizada

Un mecanismo CSPM de Security Hub al que enviar los hallazgos seleccionados. EventBridge Se crea una acción personalizada en Security Hub CSPM. A continuación, se vincula a una EventBridge regla. La regla define una acción específica que se debe realizar cuando se recibe un resultado asociado al ID de la acción personalizada. Las acciones personalizadas se pueden utilizar, por ejemplo, para enviar un resultado específico o un pequeño conjunto de resultados a un flujo de trabajo de respuesta o corrección. Para obtener más información, consulte [the section called “Crear una acción personalizada”](#).

Cuenta de administrador delegado (Organizations)

En AWS Organizations, la cuenta de administrador delegado de un servicio puede gestionar el uso de un servicio para la organización.

En Security Hub CSPM, la cuenta de administrador CSPM de Security Hub también es la cuenta de administrador delegado para Security Hub CSPM. Cuando la cuenta de administración de la organización designa por primera vez una cuenta de administrador CSPM de Security Hub, Security Hub CSPM llama a las organizaciones para convertir esa cuenta en la cuenta de administrador delegado.

A continuación, la cuenta de administración de la organización debe elegir la cuenta de administrador delegado como cuenta de administrador CSPM de Security Hub en todas las regiones.

Resultado

El registro observable de un control de seguridad o una detección relacionada con la seguridad. Security Hub CSPM genera hallazgos después de completar las comprobaciones de seguridad de los controles. Estos se denominan hallazgos de control. Los resultados también pueden provenir de integraciones con productos de otros fabricantes Servicios de AWS y de terceros.

Para obtener más información, consulte [Hallazgos del CSPM](#).

Agregación entre regiones

La agregación de resultados, información, estados de conformidad de los controles y puntuaciones de seguridad de las regiones vinculadas a una región de agregación. A continuación, puede ver todos los datos de la región de agregación y actualizar los resultados y la información de la región de agregación.

Para obtener más información, consulte [Agregación de datos del CSPM en todas las regiones](#).

Ingesta de resultados

La importación de los resultados a Security Hub CSPM desde otros AWS servicios y desde proveedores asociados externos.

Los eventos de ingesta de resultados incluyen tanto resultados nuevos como actualizaciones de resultados existentes.

Información

Una recopilación de resultados relacionados definida por una instrucción de agregación y filtros opcionales. Una información identifica un área de seguridad que requiere atención e intervención. Security Hub CSPM ofrece varios datos gestionados (predeterminados) que no se pueden modificar. También puede crear información CSPM personalizada de Security Hub para realizar un seguimiento de los problemas de seguridad que son exclusivos de su AWS entorno y uso.

Para obtener más información, consulte [Información sobre el CSPM](#).

Región vinculada

Al habilitar la agregación entre regiones, una región vinculada es una región que agrega resultados, información, estados de conformidad de controles y puntuaciones de seguridad a la región de agregación.

En una región vinculada, las páginas de Resultados e información contienen únicamente resultados de esa región.

Para obtener más información, consulte [Agregación de datos del CSPM en todas las regiones](#).

Cuenta miembro

Una cuenta que ha concedido permiso a una cuenta de administrador para ver sus resultados y tomar medidas al respecto.

Una cuenta se convierte en cuenta miembro de las siguientes formas:

- La cuenta acepta una invitación de otra cuenta.
- En el caso de una cuenta de organización, la cuenta de administrador CSPM de Security Hub habilita la cuenta como cuenta de miembro.

Requisitos relacionados

Un conjunto de requisitos reglamentarios o del sector asignados a un control.

Regla

Un conjunto de criterios automatizados que se utiliza para evaluar si se cumple un control. Cuando se evalúa una regla, puede superarse o devolver un error. Si la evaluación no puede determinar si la regla se supera o devuelve un error, la regla se encuentra en un estado de advertencia. Si la regla no se puede evaluar, está en un estado no disponible.

Control de seguridad

point-in-timeEvaluación específica de una regla comparándola con un único recurso que da como resultado unPASSED, FAILEDWARNING, o NOT_AVAILABLE un estado. La ejecución de un control de seguridad produce un resultado.

Cuenta de administrador CSPM de Security Hub

Una cuenta de organización que administra la membresía CSPM de Security Hub para una organización.

La cuenta de administración de la organización designa la cuenta de administrador CSPM de Security Hub en cada región. La cuenta de administración de la organización debe elegir la misma cuenta de administrador CSPM de Security Hub en todas las regiones.

La cuenta de administrador CSPM de Security Hub también es la cuenta de administrador delegado para Security Hub CSPM en Organizations.

La cuenta de administrador CSPM de Security Hub puede habilitar cualquier cuenta de la organización como cuenta de miembro. La cuenta de administrador CSPM de Security Hub también puede invitar a otras cuentas a ser cuentas de miembros.

Estándar de seguridad

Una instrucción publicada sobre un tema que especifica las características, normalmente medibles y en forma de controles, que deben cumplirse o lograrse para fines de conformidad. Los estándares de seguridad pueden basarse en marcos normativos, prácticas recomendadas o políticas internas de la empresa. Un control puede estar asociado a uno o más estándares compatibles en Security Hub CSPM. Para obtener más información sobre los estándares de seguridad de Security Hub CSPM, consulte [Descripción de los estándares de seguridad en Security Hub \(CSPM\)](#)

Gravedad

La gravedad asignada a un control CSPM de Security Hub identifica la importancia del control. La gravedad de un control puede ser Crítica, Alta, Media, Baja o Informativa. La gravedad asignada a los resultados del control es igual a la gravedad del propio control. Para obtener información sobre cómo el CSPM de Security Hub asigna la gravedad a un control, consulte [Niveles de gravedad de los hallazgos de control](#)

Estado del flujo de trabajo

El estado de una investigación sobre un resultado. Esto se rastrea mediante el atributo.

`Workflow.Status`

El estado del flujo de trabajo es inicialmente NEW. Si ha notificado al propietario del recurso que tome medidas sobre el resultado, puede establecer el estado del flujo de trabajo en NOTIFIED. Si el resultado no es un problema y no requiere ninguna acción, establezca el estado del flujo de trabajo en SUPPRESSED. Después de revisar y corregir un resultado, establezca el estado del flujo de trabajo en RESOLVED.

De forma predeterminada, la mayoría de las listas de resultados solo incluyen resultados con un estado de flujo de trabajo de NEW o NOTIFIED. Las listas de resultados para los controles también incluyen resultados RESOLVED.

Para la operación de [GetFindings](#), puede incluir un filtro para el estado del flujo de trabajo.

```
"WorkflowStatus": [  
  {  
    "Comparison": "EQUALS",
```

```
    "Value": "RESOLVED"  
  }  
],
```

La consola CSPM de Security Hub ofrece una opción para configurar el estado del flujo de trabajo de los hallazgos. Los clientes (o herramientas SOAR, de SIEM, de venta de tickets, de administración de incidentes que trabajan en nombre de un cliente para actualizar resultados de los proveedores de resultados) también pueden utilizar [BatchUpdateFindings](#) para actualizar el estado del flujo de trabajo.

Activación de Security Hub CSPM

Hay dos formas de habilitar la gestión de AWS la postura de seguridad (CSPM) en la nube de Security Hub: integrándolo con AWS Organizations o manualmente.

Se recomienda encarecidamente la integración con Organizations para entornos con varias cuentas y regiones. Si tiene una cuenta independiente, es necesario configurar el Security Hub CSPM manualmente.

Verificación de los permisos necesarios

Tras suscribirse a Amazon Web Services (AWS), debe habilitar Security Hub CSPM para que utilice sus funciones y funciones. Para habilitar el CSPM de Security Hub, primero debe configurar los permisos que le permitan acceder a la consola CSPM de Security Hub y a las operaciones de la API. Usted o su AWS administrador pueden hacerlo mediante AWS Identity and Access Management (IAM) para adjuntar la política AWS gestionada llamada `AWSecurityHubFullAccess` a su identidad de IAM.

Para habilitar y administrar Security Hub CSPM a través de la integración de Organizations, también debe adjuntar la política AWS administrada denominada `AWSecurityHubOrganizationsAccess`

Para obtener más información, consulte [AWS políticas gestionadas para Security Hub](#).

Habilitación de la integración de Security Hub CSPM con Organizations

Para empezar a usar Security Hub CSPM con AWS Organizations, la cuenta de AWS Organizations administración de la organización designa una cuenta como la cuenta de administrador de CSPM de Security Hub delegada para la organización. El CSPM de Security Hub se habilita automáticamente en la cuenta de administrador delegado de la región actual.

Seleccione el método que prefiera y siga los pasos para designar el administrador delegado.

Security Hub CSPM console

Para designar al administrador (CSPM) de Security Hub delegado al incorporarse

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. Seleccione Ir a Security Hub CSPM. Se le solicitará que inicie sesión en la cuenta de administración de Organizations.
3. En la página Designar administrador delegado, en la sección Cuenta de administrador delegado, especifique la cuenta de administrador delegado. Se recomienda que elija el mismo administrador delegado que haya configurado para otros servicios de seguridad y conformidad de AWS .
4. Elija Establecer administrador delegado.

Security Hub CSPM API

Invoque la API [EnableOrganizationAdminAccount](#) desde la cuenta de administración de Organizations. Proporcione el Cuenta de AWS ID de la cuenta de administrador delegado de CSPM de Security Hub.

AWS CLI

Ejecute el comando [enable-organization-admin-account](#) desde la cuenta de administración de Organizations. Proporcione el Cuenta de AWS ID de la cuenta de administrador delegado de CSPM de Security Hub.

Comando de ejemplo:

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

Para obtener más información acerca de la integración con Organizations, consulte [Integración de Security Hub CSPM con AWS Organizations](#).

Configuración centralizada

Al integrar Security Hub CSPM y Organizations, tiene la opción de usar una función llamada [configuración central](#) para configurar y administrar Security Hub CSPM para su organización.

Se recomienda encarecidamente utilizar la configuración centralizada porque permite que el administrador personalice la cobertura de seguridad de la organización. Cuando corresponde, el administrador delegado puede permitir que la cuenta de un miembro configure sus propios ajustes de cobertura de seguridad.

La configuración central permite al administrador delegado configurar Security Hub (CSPM) en todas las cuentas, y OUs. Regiones de AWS El administrador delegado configura el CSPM de Security Hub mediante la creación de políticas de configuración. Dentro de una política de configuración, puede especificar la siguiente configuración:

- Si Security Hub CSPM está activado o desactivado
- Los estándares de seguridad que se habilitan y deshabilitan
- Los controles de seguridad que se habilitan y deshabilitan
- Si se deben personalizar los parámetros de los controles seleccionados

Como administrador delegado, puede crear una política de configuración única para toda la organización o diferentes políticas de configuración para sus distintas cuentas y OUs. Por ejemplo, las cuentas de prueba y las cuentas de producción pueden utilizar políticas de configuración diferentes.

Las cuentas de los miembros OUs que utilizan una política de configuración se administran de forma centralizada y solo el administrador delegado puede configurarlas. El administrador delegado puede designar cuentas de miembros específicas y OUs autoadministrarlas para que el miembro pueda configurar sus propios ajustes de forma específica. Region-by-Region

Si no utiliza la configuración central, debe configurar en gran medida el Security Hub CSPM por separado en cada cuenta y región. Esto se denomina [configuración local](#). En la configuración local, el administrador delegado puede habilitar automáticamente el Security Hub CSPM y un conjunto limitado de estándares de seguridad en las nuevas cuentas de la organización en la región actual. La configuración local no se aplica a las cuentas de la organización existentes ni a otras regiones que no sean la actual. La configuración local tampoco admite el uso de políticas de configuración.

Activación manual del Security Hub CSPM

Debe habilitar el CSPM de Security Hub manualmente si tiene una cuenta independiente o si no se integra con ella. AWS Organizations Las cuentas independientes no se pueden integrar con la activación manual AWS Organizations y deben utilizarla.

Al activar Security Hub CSPM manualmente, designa una cuenta de administrador de Security Hub CSPM e invita a otras cuentas a convertirse en cuentas de miembros. La relación entre administrador y miembros se establece cuando una potencial cuenta de miembro acepta la invitación.

Elija el método que prefiera y siga los pasos para activar el CSPM de Security Hub. Al habilitar Security Hub CSPM desde la consola, también tiene la opción de habilitar los estándares de seguridad compatibles.

Security Hub CSPM console

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
2. Cuando abra la consola CSPM de Security Hub por primera vez, elija Ir a Security Hub CSPM.
3. En la página de bienvenida, la sección Estándares de seguridad enumera los estándares de seguridad compatibles con Security Hub CSPM.

Seleccione la casilla de verificación de un estándar para habilitarlo y quite la selección de la casilla para deshabilitarlo.

Puede habilitar o deshabilitar un estándar o sus controles individuales en cualquier momento. Para obtener más información sobre cómo administrar los estándares de seguridad, consulte [Descripción de los estándares de seguridad en Security Hub \(CSPM\)](#).

4. Seleccione Habilitar Security Hub.

Security Hub CSPM API

invoque la API [EnableSecurityHub](#). Al habilitar el CSPM de Security Hub desde la API, se habilitan automáticamente los siguientes estándares de seguridad predeterminados:

- AWS Mejores prácticas de seguridad fundamentales
- Punto de referencia básico del Center for Internet Security (CIS), AWS versión 1.2.0

Si no deseas habilitar estos estándares, establece `EnableDefaultStandards` como `false`.

También puede usar el parámetro `Tags` para asignar valores de etiqueta al recurso del hub.

AWS CLI

Ejecute el comando [enable-security-hub](#). Para habilitar los estándares predeterminados, incluya `--enable-default-standards`. Para no habilitar los estándares predeterminados, incluya `--no-enable-default-standards`. Los estándares de seguridad predeterminados son los siguientes:

- AWS Mejores prácticas fundamentales de seguridad
- Punto de referencia básico del Center for Internet Security (CIS), AWS versión 1.2.0

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-standards | --no-enable-default-standards]
```

Ejemplo

```
aws securityhub enable-security-hub --enable-default-standards --tags '{"Department": "Security"}'
```

Script de habilitación de múltiples cuentas

Note

En lugar de este script, recomendamos usar la configuración central para habilitar y configurar Security Hub CSPM en varias cuentas y regiones.

El [script de activación de múltiples cuentas de Security Hub CSPM GitHub le permite habilitar el CSPM de Security Hub en](#) todas las cuentas y regiones. El script también automatiza el proceso de envío de invitaciones a las cuentas miembro y de activación de AWS Config.

El script permite registrar automáticamente los recursos de todos los AWS Config recursos, incluidos los globales, en todas las regiones. No limita el registro de recursos globales a una única región. Para ahorrar costes, recomendamos registrar los recursos globales en una sola región únicamente. Si utiliza una configuración central o una agregación entre regiones, esta debería ser su región de origen. Para obtener más información, consulte [Registrar los recursos en AWS Config](#).

Existe un script correspondiente para deshabilitar el CSPM de Security Hub en todas las cuentas y regiones.

Próximos pasos: gestión de la postura e integraciones

Tras activar Security Hub CSPM, le recomendamos que active los estándares y controles de seguridad para supervisar su postura de seguridad. Después de habilitar los controles, Security Hub CSPM comienza a ejecutar comprobaciones de seguridad y a generar resultados de control que le ayudan a detectar errores de configuración en su entorno. AWS Para recibir los resultados de control, debe habilitar y configurar AWS Config Security Hub CSPM. Para obtener más información, consulte [Habilitación y configuración AWS Config de Security Hub CSPM](#).

Tras activar Security Hub CSPM, también puede aprovechar las integraciones entre Security Hub CSPM y soluciones de otros fabricantes para ver sus Servicios de AWS resultados en Security Hub CSPM. Security Hub CSPM agrega los hallazgos de diferentes fuentes y los ingiere en un formato coherente. Para obtener más información, consulte [Descripción de las integraciones en Security Hub CSPM](#).

Habilitación y configuración AWS Config de Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (CSPM) utiliza AWS Config reglas para ejecutar comprobaciones de seguridad y generar resultados para la mayoría de los controles. AWS Config proporciona una vista detallada de la configuración de los AWS recursos de su. Cuenta de AWS Utiliza reglas para establecer una configuración de referencia para los recursos y un registrador de configuración para detectar si un recurso concreto infringe las condiciones de una regla. Algunas reglas, AWS Config denominadas reglas administradas, están predefinidas y desarrolladas por AWS Config. Otras reglas son reglas AWS Config personalizadas que desarrolla Security Hub CSPM.

AWS Config las reglas que Security Hub CSPM utiliza para los controles se denominan reglas vinculadas a servicios. Las reglas vinculadas a servicios permiten Servicios de AWS , como Security Hub (CSPM), crear AWS Config reglas en tu cuenta.

Para recibir los resultados de control en Security Hub CSPM, debe habilitar AWS Config en su cuenta y activar el registro de los recursos que evalúen sus controles habilitados. En esta página se explica cómo habilitar el CSPM AWS Config para Security Hub y activar el registro de recursos.

Consideraciones antes de habilitar y configurar AWS Config

Para recibir los resultados de control en Security Hub CSPM, su cuenta debe tener AWS Config habilitada cada una de las ubicaciones en las Región de AWS que Security Hub CSPM esté habilitado. Si utiliza Security Hub CSPM para un entorno de varias cuentas, AWS Config debe estar habilitado en cada región para la cuenta de administrador y todas las cuentas de los miembros.

Le recomendamos encarecidamente que active el registro de recursos AWS Config antes de activar los estándares y controles CSPM de Security Hub. Esto le ayuda a garantizar que los resultados de sus controles sean precisos.

Para activar el registro de recursos AWS Config, debe tener permisos suficientes para registrar los recursos en la función AWS Identity and Access Management (IAM) asociada al grabador de configuración. Además, asegúrese de que no se administre ninguna política de IAM AWS Organizations que AWS Config impida tener permiso para registrar sus recursos. Las comprobaciones de control CSPM de Security Hub evalúan la configuración de un recurso directamente y no tienen en cuenta AWS Organizations las políticas. Para obtener más información sobre la AWS Config grabación, consulte [Trabajar con la grabadora de configuración](#) en la Guía AWS Config para desarrolladores.

Si habilita un estándar en Security Hub CSPM pero no lo ha habilitado AWS Config, Security Hub CSPM intentará crear AWS Config reglas de acuerdo con la siguiente programación:

- El día en que active el estándar.
- Al día siguiente de activar el estándar.
- Tres días después de activar el estándar.
- 7 días después de activar el estándar y, a partir de entonces, de forma continua cada 7 días.

Si utiliza la configuración central, el Security Hub CSPM también intenta crear AWS Config reglas vinculadas a servicios cada vez que asocia una política de configuración que habilita uno o más estándares con las cuentas, las unidades organizativas (OUs) o la raíz.

Registrar los recursos en AWS Config

Al habilitarla AWS Config, debe especificar qué AWS recursos desea que grabe la grabadora de AWS Config configuración. A través de las reglas vinculadas al servicio, el grabador de configuración permite que Security Hub CSPM detecte cambios en las configuraciones de sus recursos.

Para que Security Hub CSPM genere resultados de control precisos, debe activar el registro de los recursos que corresponden a los controles habilitados. AWS Config Se trata principalmente de controles habilitados con un tipo de programa activado por cambios que requieren el registro de recursos. Algunos controles con un tipo de programación periódica también requieren el registro de recursos. Para obtener una lista de estos controles y sus recursos correspondientes, consulte [AWS Config Recursos necesarios para los hallazgos de control](#).

 Warning

Si no configura la AWS Config grabación correctamente para los controles CSPM de Security Hub, se pueden producir resultados de control imprecisos, especialmente en los siguientes casos:

- Nunca registró el recurso para un control determinado o deshabilitó el registro de un recurso antes de crear ese tipo de recurso. En estos casos, recibirá una confirmación WARNING sobre el control en cuestión, aunque es posible que haya creado recursos en el ámbito del control después de deshabilitar la grabación. Este WARNING resultado es un resultado predeterminado que en realidad no evalúa el estado de configuración del recurso.
- Se deshabilita la grabación de un recurso evaluado por un control concreto. En este caso, Security Hub CSPM conserva las conclusiones de control que se generaron antes de deshabilitar la grabación, aunque el control no evalúe los recursos nuevos o actualizados. Security Hub CSPM también cambia el estado de cumplimiento de las conclusiones a. WARNING Es posible que estos hallazgos retenidos no reflejen con precisión el estado de configuración actual de un recurso.

De forma predeterminada, AWS Config registra todos los recursos regionales compatibles que descubre en el entorno Región de AWS en el que se está ejecutando. Para recibir todos los resultados de control de CSPM de Security Hub, también debe configurarlo AWS Config para registrar los recursos globales. Para ahorrar costes, recomendamos registrar los recursos globales en una sola región únicamente. Si utiliza la configuración central o la agregación entre regiones, esta región debe ser su región de origen.

En AWS Config, puede elegir entre la grabación continua o la grabación diaria de los cambios en el estado de los recursos. Si elige el registro diario, AWS Config entrega los datos de configuración de los recursos al final de cada período de 24 horas si se producen cambios en el estado de los recursos. Si no hay cambios, no se entrega ningún dato. Esto puede retrasar la generación de las

conclusiones del CSPM de Security Hub para los controles activados por cambios hasta que se complete un período de 24 horas.

Para obtener más información sobre la AWS Config grabación, consulte los recursos de grabación en la Guía para [desarrolladores AWS](#).AWS Config

Formas de habilitar y configurar AWS Config

Puede habilitar AWS Config y activar el registro de recursos de cualquiera de las siguientes maneras:

- **AWS Config consola:** puedes habilitar AWS Config una cuenta mediante la AWS Config consola. Para obtener instrucciones, consulte [Configuración AWS Config con la consola](#) en la Guía para AWS Config desarrolladores.
- **AWS CLI o bien SDKs:** puede habilitar AWS Config una cuenta mediante AWS Command Line Interface (AWS CLI). Para obtener instrucciones, consulte [Configuración AWS Config con el AWS CLI](#) en la Guía para AWS Config desarrolladores. AWS Los kits de desarrollo de software (SDKs) también están disponibles para muchos lenguajes de programación.
- **CloudFormation plantilla:** AWS Config para habilitarla en varias cuentas, le recomendamos que utilice la AWS CloudFormation plantilla denominada Enable AWS Config. Para acceder a esta plantilla, consulte [las plantillas AWS CloudFormation StackSet de muestra](#) en la Guía del AWS CloudFormation usuario.

De forma predeterminada, esta plantilla excluye la grabación de los recursos globales de IAM. Asegúrese de activar la grabación para los recursos globales de IAM solo en uno de ellos Región de AWS para ahorrar costes de grabación. Si tiene habilitada la agregación entre regiones, esta debería ser la región de origen [de Security Hub CSPM](#). De lo contrario, puede ser cualquier región en la que esté disponible el CSPM de Security Hub que admita el registro de los recursos globales de IAM. Recomendamos ejecutar uno StackSet para registrar todos los recursos, incluidos los recursos globales de IAM, de la región de origen o de otra región seleccionada. A continuación, ejecute un segundo StackSet para registrar todos los recursos, excepto los recursos globales de IAM en otras regiones.

- **GitHub script:** Security Hub CSPM ofrece un [GitHubscript](#) que habilita Security Hub CSPM y AWS Config para múltiples cuentas en todas las regiones. Este script es útil si no te has integrado en una organización AWS Organizations o tienes algunas cuentas de miembros que no forman parte de ella.

Para obtener más información, consulte la siguiente entrada del blog de AWS seguridad: [Optimice AWS Config for AWS Security Hub Cloud Security Posture Management \(CSPM\) para gestionar eficazmente su postura de seguridad en la nube.](#)

Control de configuración 1

En Security Hub CSPM, el control [Config.1](#) genera FAILED resultados en su cuenta si está deshabilitado. AWS Config También genera FAILED resultados en tu cuenta si AWS Config está activado, pero el registro de recursos no está activado.

Si AWS Config está habilitado y el registro de recursos está activado, pero el registro de recursos no está activado para un tipo de recurso que comprueba un control habilitado, Security Hub CSPM genera una FAILED búsqueda para el control Config.1. Además de este FAILED hallazgo, Security Hub CSPM genera WARNING hallazgos para el control habilitado y los tipos de recursos que comprueba el control. Por ejemplo, si habilita el control [KMS.5](#) y el registro de recursos no está activado AWS KMS keys, Security Hub CSPM generará una FAILED búsqueda para el control Config.1. Security Hub CSPM también genera WARNING resultados para el control KMS.5 y sus claves KMS.

Para recibir una PASSED búsqueda del control Config.1, active el registro de recursos para todos los tipos de recursos que correspondan a los controles habilitados. Deshabilite también los controles que no sean necesarios para su organización. Esto ayuda a garantizar que no haya brechas de configuración en las comprobaciones de control de seguridad. También ayuda a garantizar que reciba información precisa sobre los recursos mal configurados.

Si es el administrador delegado de CSPM de Security Hub para una organización, el AWS Config registro debe estar configurado correctamente para su cuenta y las cuentas de sus miembros. Si utiliza la agregación entre regiones, la AWS Config grabación debe configurarse correctamente en la región de origen y en todas las regiones vinculadas. No es necesario registrar los recursos globales en las regiones vinculadas.

Generación de reglas vinculadas a servicios

Para cada control que utilice una AWS Config regla vinculada a un servicio, Security Hub CSPM crea instancias de la regla requerida en su entorno. AWS

Estas reglas vinculadas a servicios son específicas de Security Hub CSPM. Security Hub CSPM crea estas reglas vinculadas a servicios incluso si ya existen otras instancias de las mismas reglas. La regla vinculada al servicio se agrega `securityhub` antes del nombre de la regla original y un

identificador único después del nombre de la regla. Por ejemplo, en el caso de la regla AWS Config administrada `vpc-flow-logs-enabled`, el nombre de la regla vinculada al servicio podría ser `securityhub-vpc-flow-logs-enabled-12345`.

Hay cuotas para el número de reglas AWS Config administradas que se pueden usar para evaluar los controles. AWS Config las reglas que crea Security Hub CSPM no cuentan para esas cuotas. Puedes habilitar un estándar de seguridad incluso si ya has alcanzado la AWS Config cuota de reglas administradas en tu cuenta. Para obtener más información sobre las cuotas de AWS Config las reglas, consulta [los límites de servicio AWS Config en la Guía para AWS Config](#) desarrolladores.

Consideraciones sobre costos

El CSPM de Security Hub puede afectar a los costes de AWS Config la grabadora de configuración al actualizar el elemento de `AWS::Config::ResourceCompliance` configuración. Las actualizaciones se pueden producir cada vez que un control CSPM de Security Hub asociado a una AWS Config regla cambia de estado de conformidad, se habilita o deshabilita, o se actualiza los parámetros. Si usa la grabadora de AWS Config configuración solo para Security Hub CSPM y no usa este elemento de configuración para otros fines, le recomendamos que desactive la grabación. AWS Config Esto puede reducir sus costos de AWS Config . No necesita grabar las comprobaciones de seguridad `AWS::Config::ResourceCompliance` para que funcionen en Security Hub CSPM.

[Para obtener información sobre los costes asociados al registro de recursos, consulte Precios y AWS Config precios de AWS Security Hub Cloud Security Posture Management \(CSPM\).](#)

Descripción de la configuración local en Security Hub (CSPM)

La configuración local es la forma predeterminada en que se configura una AWS organización en Security Hub CSPM. Si no opta por la configuración centralizada ni la habilita, su organización utilizará la configuración local de forma predeterminada.

En la configuración local, la cuenta de administrador CSPM de Security Hub delegada tiene un control limitado sobre los ajustes de configuración. La única configuración que el administrador delegado puede aplicar es habilitar automáticamente el Security Hub CSPM y los estándares de seguridad predeterminados en las nuevas cuentas de la organización. Estos ajustes solo se aplican en la región en la que designó la cuenta de administrador delegado. Los estándares de seguridad predeterminados son AWS Foundational Security Best Practices (FSBP) y Center for Internet Security (CIS) Foundations Benchmark v1.2.0. AWS Los ajustes de configuración local no se aplican a las cuentas de la organización existentes ni a regiones distintas de aquella en la que se designó la cuenta de administrador delegado.

Además de habilitar el CSPM y los estándares predeterminados de Security Hub en las nuevas cuentas de la organización en una sola región, debe configurar otros ajustes de CSPM de Security Hub, incluidos los estándares y los controles, por separado en cada región y cuenta. Dado que este proceso puede duplicarse, le recomendamos que utilice la configuración centralizada para un entorno de varias cuentas si se presentan una o más de las siguientes situaciones:

- Quiere establecer distintos ajustes para las distintas partes de la organización (por ejemplo, distintos estándares o controles habilitados para los diferentes equipos).
- Trabaja en varias regiones y desea reducir el tiempo y la complejidad de la configuración del servicio en esas regiones.
- Desea que las cuentas nuevas usen ajustes específicos cuando se unan a la organización.
- Desea que las cuentas de la organización hereden ajustes específicos de una cuenta principal o raíz.

Para obtener información acerca de la configuración centralizada, consulte [Descripción de la configuración central en Security Hub \(CSPM\)](#).

Descripción de la configuración central en Security Hub (CSPM)

La configuración central es una función AWS de gestión de la postura de seguridad (CSPM) de Security Hub Cloud que le ayuda a configurar y administrar el Security Hub CSPM en múltiples y. Cuentas de AWS Regiones de AWS Para utilizar la configuración central, primero debe integrar Security Hub CSPM y. AWS Organizations Puede integrar los servicios creando una organización y designando una cuenta de administrador de CSPM de Security Hub delegada para la organización.

Desde la cuenta de administrador CSPM de Security Hub delegada, puede habilitar Security Hub CSPM para las cuentas y unidades organizativas () de su organización en todas las regiones. OUs También puede activar, configurar y deshabilitar los estándares de seguridad y los controles de seguridad individuales para las cuentas y las distintas regiones. OUs Puede configurar estos ajustes en tan solo unos pasos desde una región principal, denominada región de origen.

Al utilizar la configuración central, el administrador delegado puede elegir qué cuentas desea OUs configurar. Si el administrador delegado designa una cuenta de miembro o una unidad organizativa como autoadministrada, el miembro puede configurar sus propios ajustes por separado en cada región. Si el administrador delegado designa una cuenta de miembro o una unidad organizativa como administrada de forma centralizada, solo el administrador delegado puede configurar la cuenta de miembro o la unidad organizativa en todas las regiones. Puede designar todas las cuentas de

su organización como administradas de forma centralizada, todas autogestionadas o como una combinación de ambas. OUs

Para configurar las cuentas gestionadas de forma centralizada, el administrador delegado utiliza las políticas de configuración CSPM de Security Hub. Las políticas de configuración permiten al administrador delegado especificar si Security Hub CSPM está habilitado o deshabilitado y qué estándares y controles están habilitados o deshabilitados. También se pueden usar para personalizar los parámetros de determinados controles.

Las políticas de configuración entran en vigor en la región de origen y en todas las regiones vinculadas. El administrador delegado especifica la región de origen de la organización y las regiones vinculadas antes de empezar a utilizar la configuración centralizada. La especificación de las regiones vinculadas es opcional. El administrador delegado puede crear una política de configuración única para toda la organización o crear varias políticas de configuración para configurar ajustes variables para diferentes cuentas y OUs.

Tip

Si no utiliza la configuración central, debe configurar en gran medida el Security Hub CSPM por separado en cada cuenta y región. Esto se denomina configuración local. En la configuración local, el administrador delegado puede habilitar automáticamente el Security Hub CSPM y un conjunto limitado de estándares de seguridad en las nuevas cuentas de la organización en la región actual. La configuración local no se aplica a las cuentas de la organización existentes ni a otras regiones que no sean la actual. La configuración local tampoco admite el uso de políticas de configuración.

En esta sección, se proporciona información general acerca de la configuración centralizada.

Beneficios de usar la configuración centralizada

Entre los beneficios de la configuración centralizada, se incluyen los siguientes:

Simplifique la configuración del servicio y las capacidades del Security Hub CSPM

Cuando utiliza la configuración central, Security Hub CSPM lo guía a través del proceso de configuración de las mejores prácticas de seguridad para su organización. También implementa las políticas de configuración resultantes en cuentas específicas y de forma automática. OUs Si tiene una configuración de CSPM de Security Hub existente, como la activación automática

de nuevos controles de seguridad, puede utilizarla como punto de partida para sus políticas de configuración. Además, la página de configuración de la consola CSPM de Security Hub muestra un resumen en tiempo real de las políticas de configuración y de las cuentas que OUs utilizan cada política.

Configuración en todas las cuentas y regiones

Puede usar la configuración central para configurar Security Hub CSPM en varias cuentas y regiones. Esto ayuda a garantizar que cada parte de la organización mantenga una configuración coherente y una cobertura de seguridad adecuada.

Se adaptan a diferentes configuraciones en diferentes cuentas y OUs

Con la configuración central, puede elegir configurar las cuentas de su organización de diferentes OUs maneras. Por ejemplo, las cuentas de prueba y de producción pueden utilizar políticas de configuración diferentes. También puede crear una política de configuración que cubra las cuentas nuevas cuando se unan a la organización.

Prevención de desviaciones de la configuración

La desviación de la configuración ocurre cuando un usuario hace un cambio en un servicio o característica que entra en conflicto con las selecciones del administrador delegado. La configuración centralizada evita esta desviación. Cuando se designa una cuenta o unidad organizativa como administrada de forma centralizada, solo el administrador delegado de la organización puede configurarla. Si prefiere que una cuenta o unidad organizativa específica configure sus propios ajustes, puede designarla como autoadministrada.

¿Cuándo se debe utilizar la configuración centralizada?

La configuración central es más beneficiosa para los AWS entornos que incluyen varias cuentas CSPM de Security Hub. Está diseñado para ayudarle a gestionar de forma centralizada el Security Hub CSPM para varias cuentas.

Puede utilizar la configuración central para configurar el servicio CSPM de Security Hub, los estándares de seguridad y los controles de seguridad. También pueden utilizarla para personalizar los parámetros de determinados controles. Para obtener más información sobre los estándares de seguridad, consulte [Descripción de los estándares de seguridad en Security Hub \(CSPM\)](#). Para más información sobre los controles de seguridad, consulte [Descripción de los controles de seguridad en Security Hub CSPM](#).

Términos y conceptos de la configuración centralizada

Comprender los siguientes términos y conceptos clave puede ayudarle a utilizar la configuración central de Security Hub CSPM.

Configuración centralizada

Una función CSPM de Security Hub que ayuda a la cuenta de administrador de CSPM de Security Hub delegada de una organización a configurar el servicio CSPM del Security Hub, los estándares de seguridad y los controles de seguridad en varias cuentas y regiones. Para configurar estos ajustes, el administrador delegado crea y administra las políticas de configuración de CSPM de Security Hub para las cuentas administradas de forma centralizada en su organización. Las cuentas autoadministradas pueden configurar sus propios ajustes por separado en cada región. Para utilizar la configuración central, debe integrar Security Hub CSPM y. AWS Organizations

Región de origen

Región de AWS Desde el que el administrador delegado configura centralmente el Security Hub CSPM, mediante la creación y administración de políticas de configuración. Las políticas de configuración entran en vigor en la región de origen y en todas las regiones vinculadas.

La región de origen también actúa como región de agregación de CSPM del Security Hub y recibe hallazgos, información y otros datos de las regiones vinculadas.

Las regiones que AWS se introdujeron el 20 de marzo de 2019 o después se denominan regiones con suscripción voluntaria. Una región optativa no puede ser la región de origen, pero puede ser una región vinculada. Para ver una lista de las regiones opcionales, consulte la sección [Considerations before enabling and disabling Regions](#) en la Guía de referencia de administración de cuentas de AWS .

Región vinculada

Y Región de AWS que se pueden configurar desde la región de origen. El administrador delegado crea las políticas de configuración en la región de origen. Las políticas entran en vigor en la región de origen y en todas las regiones vinculadas. La especificación de las regiones vinculadas es opcional.

Una región vinculada también envía resultados, información y otros datos a la región de origen.

Las regiones que AWS se introdujeron el 20 de marzo de 2019 o después se conocen como regiones con suscripción voluntaria. Debe habilitar dicha región para una cuenta antes de poder

aplicarle una política de configuración. La cuenta de administración de Organizations puede habilitar regiones optativas para una cuenta de miembro. Para obtener más información, consulta [Especificar qué Regiones de AWS cuenta puedes usar](#) en la Guía de referencia de administración de AWS cuentas.

Destino

Una Cuenta de AWS unidad organizativa (OU) o la raíz de la organización.

Política de configuración CSPM de Security Hub

Un conjunto de ajustes de CSPM de Security Hub que el administrador delegado puede configurar para los destinos gestionados de forma centralizada. Esto incluye:

- Si se debe habilitar o deshabilitar Security Hub CSPM.
- Si se habilitan uno o más [estándares de seguridad](#).
- Qué [controles de seguridad](#) se habilitan en todos los estándares habilitados. El administrador delegado puede hacerlo proporcionando una lista de controles específicos que deben habilitarse, y Security Hub CSPM deshabilita todos los demás controles (incluidos los controles nuevos cuando se publican). Como alternativa, el administrador delegado puede proporcionar una lista de controles específicos que deben deshabilitarse y Security Hub CSPM habilita todos los demás controles (incluidos los nuevos controles cuando se publiquen).
- Si lo desea, [personalice parámetros](#) de ciertos controles habilitados en los estándares habilitados.

Una política de configuración entra en vigor en la región de origen y en todas las regiones vinculadas una vez que se ha asociado al menos a una cuenta, una unidad organizativa (OU) o la raíz.

En la consola CSPM de Security Hub, el administrador delegado puede elegir la política de configuración recomendada de Security Hub CSPM o crear políticas de configuración personalizadas. Con la API CSPM de Security Hub y AWS CLI, el administrador delegado solo puede crear políticas de configuración personalizadas. El administrador delegado puede crear un máximo de 20 políticas de configuración personalizadas.

En la política de configuración recomendada, el Security Hub CSPM, el estándar AWS Foundational Security Best Practices (FSBP) y todos los controles FSBP nuevos y existentes están habilitados. Los controles que aceptan parámetros utilizan los valores predeterminados. La política de configuración recomendada se aplica a toda la organización.

Para aplicar diferentes ajustes a la organización o aplicar diferentes políticas de configuración a diferentes cuentas y OUs crear una política de configuración personalizada.

Configuración local

El tipo de configuración predeterminado para una organización, después de integrar Security Hub CSPM y AWS Organizations Con la configuración local, el administrador delegado puede optar por habilitar automáticamente el Security Hub CSPM y los [estándares de seguridad predeterminados](#) en las nuevas cuentas de la organización en la región actual. Si el administrador delegado habilita automáticamente los estándares predeterminados, todos los controles que forman parte de estos estándares también se habilitan automáticamente con los parámetros predeterminados para las nuevas cuentas de la organización. Esa configuración no se aplica a las cuentas existentes, por lo que es posible que se modifique la configuración una vez que una cuenta se una a la organización. La deshabilitación de controles específicos que forman parte de los estándares predeterminados y la configuración de estándares y controles adicionales deben llevarse a cabo por separado en cada cuenta y región.

La configuración local no admite el uso de políticas de configuración. Para usar las políticas de configuración, debe cambiar a la configuración centralizada.

Administración manual de cuentas

Si no integra Security Hub CSPM AWS Organizations o tiene una cuenta independiente, debe especificar la configuración de cada cuenta por separado en cada región. La administración manual de cuentas no admite el uso de políticas de configuración.

Configuración centralizada APIs

Operaciones de CSPM del Security Hub que solo el administrador del Security Hub CSPM delegado por el Security Hub CSPM puede utilizar en la región de origen para gestionar las políticas de configuración de las cuentas gestionadas de forma centralizada. Las operaciones incluyen:

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`

- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

Cuenta específica APIs

Operaciones de CSPM de Security Hub que se pueden utilizar para habilitar o deshabilitar el CSPM, los estándares y los controles de Security Hub de forma independiente. account-by-account Estas operaciones se utilizan en cada región individual.

Las cuentas autoadministradas pueden utilizar operaciones específicas de la cuenta para configurar sus propios ajustes. Las cuentas administradas de forma centralizada no pueden llevar a cabo las siguientes operaciones específicas de la cuenta en la región de origen y en las regiones vinculadas. En esas regiones, solo el administrador delegado puede configurar las cuentas administradas de forma centralizada mediante operaciones de configuración y políticas de configuración centralizadas.

- `BatchDisableStandards`
- `BatchEnableStandards`
- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`
- `EnableSecurityHub`
- `UpdateStandardsControl`

Para comprobar el estado de la cuenta, el propietario de una cuenta gestionada de forma centralizada puede utilizar cualquiera `Get` de `Describe` las operaciones de la API CSPM de Security Hub.

Si utiliza la configuración local o la administración manual de la cuenta, en lugar de la configuración centralizada, puede utilizar estas operaciones específicas de la cuenta.

Las cuentas autoadministradas también pueden utilizar las operaciones `*Invitations` y `*Members`. Sin embargo, recomendamos que las cuentas autoadministradas no utilicen estas operaciones. Las asociaciones de políticas pueden fallar si la cuenta de miembro tiene sus propios miembros que forman parte de una organización diferente a la del administrador delegado.

Unidad organizativa (OU)

En AWS Organizations Security Hub CSPM, un contenedor para un grupo de. Cuentas de AWS Una unidad organizativa (OU) también puede contener otras OUs, lo que permite crear una jerarquía similar a un árbol invertido, con una unidad organizativa principal en la parte superior y con las ramas extendidas hacia abajo y acabando en cuentas que son las hojas del árbol. OUs Una unidad organizativa puede tener una unidad principal y cada cuenta de la organización puede ser miembro de exactamente una unidad organizativa.

Puede administrar OUs en AWS Organizations o. AWS Control Tower Para obtener más información, consulte [Administración de unidades organizativas](#) en la Guía del usuario de AWS Organizations o [Control de organizaciones y cuentas con AWS Control Tower](#) en la Guía del usuario de AWS Control Tower .

El administrador delegado puede asociar las políticas de configuración a cuentas específicas o OUs a la raíz para abarcar todas las cuentas OUs de una organización.

Administrada de forma centralizada

Un destino que solo el administrador delegado puede configurar en todas las regiones mediante políticas de configuración.

La cuenta de administrador delegado especifica si un destino se administra de forma centralizada. El administrador delegado también puede cambiar el estado del destino de administrado centralmente a autoadministrado o al revés.

Autoadministrado

Un objetivo que administra su propia configuración de CSPM de Security Hub. Un objetivo autogestionado utiliza operaciones específicas de la cuenta para configurar el CSPM de Security Hub por separado en cada región. Esto contrasta con los destinos administrados de forma centralizada, que solo el administrador delegado puede configurar en todas las regiones mediante políticas de configuración.

La cuenta de administrador delegado especifica si un destino es autoadministrado. El administrador delegado puede aplicar un comportamiento autoadministrado a un destino. Como alternativa, una cuenta o unidad organizativa pueden heredar el comportamiento autoadministrado de una unidad principal.

La cuenta de administrador delegado en sí puede ser una cuenta autoadministrada. La cuenta de administrador delegado puede cambiar el estado de un destino, de autoadministrado a administrado de forma centralizada o al revés.

Asociación de políticas de configuración

Enlace entre una política de configuración y una cuenta, unidad organizativa (OU) o raíz. Cuando existe una asociación de políticas, la cuenta, la unidad organizativa o la cuenta raíz utiliza los parámetros definidos en la política de configuración. Existe una asociación en cualquiera de estos casos:

- Cuando el administrador delegado aplica directamente una política de configuración a una cuenta, unidad organizativa o raíz
- Cuando una cuenta o unidad organizativa hereda una política de configuración de una unidad organizativa principal o de la cuenta raíz

Existe una asociación hasta que se aplique o herede una configuración diferente.

Política de configuración aplicada

Tipo de asociación de políticas de configuración en la que el administrador delegado aplica directamente una política de configuración a las cuentas de destino o a la raíz. Los destinos se configuran de la manera que define la política de configuración y solo el administrador delegado puede cambiar su configuración. Si se aplica a la raíz, la política de configuración afecta a todas las OUs cuentas de la organización que no utilicen una configuración diferente mediante la aplicación o la herencia de la empresa matriz más cercana.

El administrador delegado también puede aplicar una configuración autogestionada a cuentas específicas o a la raíz. OUs

Política de configuración heredada

Tipo de asociación de políticas de configuración en la que una cuenta o unidad organizativa adopta la configuración de la unidad organizativa principal más cercana o de la raíz. Si una política de configuración no se aplica directamente a una cuenta o unidad organizativa, hereda la configuración de la unidad principal más cercana. Todos los elementos de una política se heredan. En otras palabras, una cuenta o unidad organizativa no puede elegir si hereda solo partes de una política de forma selectiva. Si la unidad principal más cercana está autoadministrada, la cuenta secundaria o la unidad organizativa hereda el comportamiento autoadministrado de la unidad principal.

La herencia no puede anular una configuración aplicada. Es decir, si una política de configuración o una configuración autoadministrada se aplica directamente a una cuenta o unidad organizativa, utiliza esa configuración y no hereda la configuración de la unidad principal.

Raíz

En AWS Organizations Security Hub CSPM, el nodo principal de nivel superior de una organización. Si el administrador delegado aplica una política de configuración a la raíz, la política se asocia a todas las cuentas de la organización, a menos que utilicen una política diferente, por aplicación o herencia, o se OUs designen como autogestionables. Si el administrador designa la raíz como autogestionada, todas las cuentas de la organización se autogestionarán, a menos que utilicen una política de configuración por aplicación o herencia. OUs Si la raíz es autoadministrada y actualmente no existen políticas de configuración, todas las cuentas nuevas de la organización retienen su configuración actual.

Las cuentas nuevas que se unen a una organización se clasifican en la raíz hasta que se asignan a una unidad organizativa específica. Si una cuenta nueva no está asignada a una unidad organizativa, hereda la configuración raíz, a menos que el administrador delegado la designe como cuenta autoadministrada.

Activación de la configuración central en Security Hub (CSPM)

La cuenta de administrador delegada de AWS Security Hub Cloud Security Posture Management (CSPM) puede usar la configuración central para configurar el CSPM, los estándares y los controles del Security Hub para varias cuentas y unidades organizativas () en todas. OUs Regiones de AWS

Para obtener información general sobre las ventajas de la configuración centralizada y su funcionamiento, consulte [Descripción de la configuración central en Security Hub \(CSPM\)](#).

En esta sección, se explican los requisitos previos para la configuración centralizada y cómo empezar a utilizarla.

Requisitos previos para la configuración centralizada

Antes de empezar a utilizar la configuración central, debe integrar Security Hub CSPM AWS Organizations y designar una región de origen. Si utiliza la consola CSPM de Security Hub, estos requisitos previos se incluyen en el flujo de trabajo opcional para la configuración central.

Integración con Organizations

Debe integrar Security Hub CSPM y Organizations para utilizar la configuración central.

Para integrar estos servicios, comience por crear una organización en Organizations. A continuación, desde la cuenta de administración de Organizations, se designa una cuenta de administrador

delegado CSPM de Security Hub. Para obtener instrucciones, consulte [Integración de Security Hub CSPM con AWS Organizations](#).

Asegúrese de designar un administrador delegado en la región de origen prevista. Cuando empieza a utilizar la configuración centralizada, también se establece automáticamente el mismo administrador delegado en todas las regiones vinculadas. La cuenta de administración de Organizations no se puede establecer como cuenta de administrador delegado.

 Important

Cuando usa la configuración central, no puede usar la consola CSPM de Security Hub ni la CSPM de Security Hub APIs para cambiar o eliminar la cuenta de administrador delegado. Si la cuenta de administración de la organización se utiliza AWS Organizations APIs para cambiar o eliminar al administrador delegado de CSPM de Security Hub, Security Hub CSPM detiene automáticamente la configuración central. Sus políticas de configuración también se desasocian y se eliminan. Las cuentas de miembro retienen la configuración que tenían antes de que se cambiara o eliminara el administrador delegado.

Designación de una región de origen

Debe designar una región de origen para utilizar la configuración centralizada. La región de origen es aquella desde la que el administrador delegado configura la organización.

 Note

La región de origen no puede ser una región AWS designada como región opcional. Las regiones optativas están deshabilitadas de forma predeterminada. Para ver una lista de las regiones opcionales, consulte la sección [Considerations before enabling and disabling Regions](#) en la Guía de referencia de administración de cuentas de AWS .

Si lo desea, puede especificar una o más regiones vinculadas que se puedan configurar desde la región de origen.

El administrador delegado puede crear y administrar políticas de configuración solo desde la región de agregación. Las políticas de configuración entran en vigor en la región de origen y en todas las regiones vinculadas. No puede crear una política de configuración que se aplique exclusivamente a un subconjunto de estas regiones. La excepción a esto son los controles que involucran recursos

globales. Si usa la configuración central, Security Hub CSPM deshabilita automáticamente los controles que involucran recursos globales en todas las regiones, excepto en la región de origen. Para obtener más información, consulte [Controles que utilizan recursos globales](#).

La región de origen también es la región de agregación de CSPM de Security Hub que recibe hallazgos, información y otros datos de las regiones vinculadas.

Si ya ha establecido una región de agregación para la agregación entre regiones, esa será su región de origen predeterminada para la configuración centralizada. Puede cambiar la región de origen antes de empezar a utilizar la configuración centralizada. Para ello, elimine su agregador de resultados actual y cree uno nuevo en la región de origen que desee. Un agregador de búsquedas es un recurso CSPM de Security Hub que especifica la región de origen y las regiones vinculadas.

Para designar una región de origen, consulte [los pasos para configurar una región de agregación](#). Si ya tiene una región de origen, puede invocar la API [GetFindingAggregator](#) para ver los detalles de dicha región, lo que incluye las regiones que están vinculadas actualmente a ella.

Instrucciones para habilitar la configuración centralizada

Elija el método que prefiera y siga los pasos para habilitar la configuración centralizada en su organización.

Security Hub CSPM console

Para habilitar la configuración centralizada (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, seleccione Configuración y Configuración. A continuación, elija Iniciar configuración centralizada.

Si se va a incorporar a Security Hub CSPM, elija Ir a Security Hub CSPM.

3. En la página Designar administrador delegado, seleccione su cuenta de administrador delegado o ingrese su ID de cuenta. Si corresponde, se recomienda que elija el mismo administrador delegado que haya configurado para otros servicios de seguridad y conformidad de AWS. Elija Establecer administrador delegado.
4. En la página Centralizar organización, en la sección Regiones, seleccione su región de origen. Debe haber iniciado sesión en dicha región para continuar. Si ya ha configurado una región de agregación para la agregación entre regiones, aparecerá como la región de

origen. Para cambiar la región de origen, seleccione Editar configuración de la región. A continuación, puede seleccionar la región de origen que prefiera y volver a este flujo de trabajo.

5. Seleccione al menos una región para vincularla a la región de origen. De manera opcional, elija si desea vincular automáticamente las futuras regiones compatibles con la región de origen. El administrador delegado configurará las regiones que seleccione aquí desde la región de origen. Las políticas de configuración entran en vigor en la región de origen y en todas las regiones vinculadas.
6. Seleccione Confirmar y continuar.
7. A partir de ahora, puede utilizar la configuración centralizada. Siga las instrucciones de la consola para crear su primera política de configuración. Si aún no lo tiene todo preparado para crear una política de configuración, seleccione Aún no lo tengo todo listo para configurarla. Para crear una política más adelante, puede seleccionar Configuración y, a continuación, Configuración en el panel de navegación. Para obtener instrucciones sobre cómo crear una política de configuración, consulte [Creación y asociación de políticas de configuración](#).

Security Hub CSPM API

Para habilitar la configuración centralizada (API)

1. Con las credenciales de la cuenta de administrador delegado, invoque la API [UpdateOrganizationConfiguration](#) desde la región de origen.
2. Establezca el campo `AutoEnable` como `false`.
3. Establezca el campo `ConfigurationType` del objeto `OrganizationConfiguration` en `CENTRAL`. Esta acción tiene los siguientes efectos:
 - Designa la cuenta llamante como administradora delegada de CSPM de Security Hub en todas las regiones vinculadas.
 - Activa el CSPM de Security Hub en la cuenta de administrador delegado de todas las regiones vinculadas.
 - Designa la cuenta llamante como administradora delegada de CSPM de Security Hub para las cuentas nuevas y existentes que utilizan Security Hub CSPM y pertenecen a la organización. Esto ocurre en la región de origen y en todas las regiones vinculadas. La cuenta de llamada se establece como la administradora delegada para las nuevas cuentas de la organización solo si están asociadas a una política de configuración que

tenga activado el CSPM de Security Hub. La cuenta de llamada se configura como la administradora delegada de las cuentas de la organización existentes solo si ya tienen activado el CSPM de Security Hub.

- Se establece [AutoEnable](#) como `false` en todas las regiones vinculadas y se establece [AutoEnableStandards](#) como `NONE` en la región de origen y en todas las regiones vinculadas. Estos parámetros no son relevantes en las regiones de origen y vinculadas cuando se usa la configuración central, pero puede habilitar automáticamente el Security Hub CSPM y los estándares de seguridad predeterminados en las cuentas de la organización mediante el uso de políticas de configuración.
4. A partir de ahora, puede utilizar la configuración centralizada. El administrador delegado puede crear políticas de configuración para configurar Security Hub CSPM en su organización. Para obtener instrucciones sobre cómo crear una política de configuración, consulte [Creación y asociación de políticas de configuración](#).

Ejemplo de solicitud de API:

```
{
  "AutoEnable": false,
  "OrganizationConfiguration": {
    "ConfigurationType": "CENTRAL"
  }
}
```

AWS CLI

Para habilitar la configuración centralizada (AWS CLI)

1. Con las credenciales de la cuenta de administrador delegado, ejecute el comando [update-organization-configuration](#) desde la región de origen.
2. Incluya el parámetro `no-auto-enable`.
3. Establezca el campo `ConfigurationType` del objeto `organization-configuration` en `CENTRAL`. Esta acción tiene los siguientes efectos:
 - Designa la cuenta llamante como administradora delegada de CSPM de Security Hub en todas las regiones vinculadas.

- Activa el CSPM de Security Hub en la cuenta de administrador delegado de todas las regiones vinculadas.
 - Designa la cuenta llamante como administradora delegada de CSPM de Security Hub para las cuentas nuevas y existentes que utilizan Security Hub CSPM y pertenecen a la organización. Esto ocurre en la región de origen y en todas las regiones vinculadas. La cuenta que llama se establece como administrador delegado para las nuevas cuentas de la organización solo si están asociadas a una política de configuración que tenga habilitado Security Hub. La cuenta de llamada se configura como la administradora delegada de las cuentas de la organización existentes solo si ya tienen activado el CSPM de Security Hub.
 - Establece la opción de habilitación automática como [no-auto-enable](#) en todas las regiones vinculadas y establece [auto-enable-standards](#) como NONE en la región de origen y en todas las regiones vinculadas. Estos parámetros no son relevantes en las regiones de origen y vinculadas cuando se usa la configuración central, pero puede habilitar automáticamente el Security Hub CSPM y los estándares de seguridad predeterminados en las cuentas de la organización mediante el uso de políticas de configuración.
4. A partir de ahora, puede utilizar la configuración centralizada. El administrador delegado puede crear políticas de configuración para configurar Security Hub CSPM en su organización. Para obtener instrucciones sobre cómo crear una política de configuración, consulte [Creación y asociación de políticas de configuración](#).

Comando de ejemplo:

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}
```

Objetivos gestionados de forma centralizada frente a objetivos autogestionados

Al habilitar la configuración central, el administrador delegado de AWS Security Hub Cloud Security Posture Management (CSPM) puede designar cada cuenta, unidad organizativa (OU) y raíz de la organización como gestionada de forma centralizada o autogestionada. El tipo de administración de un objetivo determina cómo se puede especificar la configuración de CSPM de Security Hub.

Para obtener información general sobre las ventajas de la configuración centralizada y su funcionamiento, consulte [Descripción de la configuración central en Security Hub \(CSPM\)](#).

En esta sección se explican las diferencias entre una designación administrada de forma centralizada y una autoadministrada, y cómo elegir el tipo de administración de una cuenta, una unidad organizativa o la raíz.

Autoadministrado

El propietario de una cuenta, unidad organizativa o root autogestionada debe configurar sus ajustes por separado en cada una de ellas. Región de AWS El administrador delegado no puede crear políticas de configuración para destinos autoadministrados.

Administrada de forma centralizada

Solo el administrador CSPM de Security Hub delegado puede configurar los ajustes de las cuentas gestionadas de forma centralizada o de la raíz en la región de origen y las regiones vinculadas. OUs Las políticas de configuración se pueden asociar a cuentas administradas de forma centralizada y. OUs

El administrador delegado puede cambiar el estado de un destino entre autoadministrado y administrado de forma centralizada. De forma predeterminada, todas las cuentas y la unidad organizativa se autoadministran al iniciar la configuración central a través de la API CSPM de Security Hub. En la consola, el tipo de administración depende de la primera política de configuración. Las cuentas y las OUs que asocie a su primera política se administran de forma centralizada. El resto de las cuentas OUs se administran automáticamente de forma predeterminada.

Si asocia una política de configuración a una cuenta previamente autogestionada, los ajustes de la política anulan la designación autogestionada. La cuenta pasa a administrarse de forma centralizada y adopta los ajustes reflejados en la política de configuración.

Si cambias una cuenta gestionada de forma centralizada a una cuenta autogestionada, se mantienen los ajustes que se aplicaban anteriormente a la cuenta mediante una política de configuración. Por ejemplo, una cuenta gestionada de forma centralizada podría asociarse inicialmente a una política que habilitara el CSPM de Security Hub, habilitara las prácticas recomendadas de seguridad AWS fundamentales y deshabilitara .1. CloudTrail Si, a continuación, designa la cuenta como autogestionada, todos los ajustes permanecerán inalterados. Sin embargo, el propietario de la cuenta puede cambiar de forma independiente la configuración de la cuenta en el futuro.

Las cuentas secundarias OUs pueden heredar el comportamiento autogestionado de una entidad matriz autogestionada, del mismo modo que las cuentas secundarias, y OUs pueden heredar las políticas de configuración de una entidad matriz gestionada de forma centralizada. Para obtener más información, consulte [Asociación de políticas mediante la aplicación y la herencia](#).

Una cuenta o una unidad organizativa autoadministrada no puede heredar una política de configuración de un nodo principal o de la raíz. Por ejemplo, si desea que todas las cuentas de su organización hereden una política de configuración de la raíz, debe cambiar el tipo de administración de los nodos autogestionados a gestionados de forma centralizada. OUs

Opciones para configurar los ajustes en las cuentas autoadministradas

Las cuentas autoadministradas deben configurar sus ajustes por separado en cada región.

Los propietarios de cuentas autogestionadas pueden invocar las siguientes operaciones de la API CSPM de Security Hub en cada región para configurar sus ajustes:

- `EnableSecurityHub` y `DisableSecurityHub` para habilitar o deshabilitar el servicio CSPM de Security Hub (si una cuenta autogestionada tiene un administrador de CSPM de Security Hub delegado, el administrador [debe desasociar la cuenta antes de que el propietario de la](#) cuenta pueda deshabilitar Security Hub CSPM).
- `BatchEnableStandards` y `BatchDisableStandards` para habilitar o deshabilitar estándares
- `BatchUpdateStandardsControlAssociations` o `UpdateStandardsControl` para habilitar o deshabilitar controles

Las cuentas autoadministradas también pueden utilizar las operaciones `*Invitations` y `*Members`. Sin embargo, recomendamos que las cuentas autoadministradas no utilicen estas operaciones. Las asociaciones de políticas pueden fallar si la cuenta de miembro tiene sus propios miembros que forman parte de una organización diferente a la del administrador delegado.

Para obtener descripciones de las acciones de la API CSPM de Security Hub, consulte la referencia de la AWS API de [administración de posturas de seguridad \(CSPM\) de Security Hub Cloud](#).

Las cuentas autogestionadas también pueden usar la consola CSPM de Security Hub o AWS CLI para configurar sus ajustes en cada región.

Las cuentas autogestionadas no pueden invocar ninguna política de configuración o asociación de políticas de CSPM APIs relacionada con Security Hub. Solo el administrador delegado puede invocar

la configuración central APIs y utilizar las políticas de configuración para configurar las cuentas gestionadas de forma centralizada.

Elección del tipo de administración de un destino

Elija el método que prefiera y siga los pasos para designar una cuenta o unidad organizativa como gestionada de forma centralizada o autogestionada en AWS Security Hub Cloud Security Posture Management (CSPM).

Security Hub CSPM console

Elección del tipo de administración de una cuenta o unidad organizativa

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>.

Inicie sesión con las credenciales de la cuenta de administrador CSPM de Security Hub delegada en la región de origen.
2. Elija Configuración.
3. En la pestaña Organización, seleccione la cuenta o la unidad organizativa de destino. Seleccione Editar.
4. En la página Definir configuración, en Tipo de administración, elija Administrada de forma centralizada si desea que el administrador delegado configure la cuenta o unidad organizativa de destino. A continuación, elija Aplicar una política específica si desea asociar una política de configuración existente al destino. Elija Heredar de mi organización si desea que el destino herede la configuración de la cuenta principal más cercana. Elija Autoadministrado si desea que la cuenta o unidad organizativa configure sus propios ajustes.
5. Elija Siguiente. Revise los cambios y seleccione Guardar.

Security Hub CSPM API

Elección del tipo de administración de una cuenta o unidad organizativa

1. Invoque la [StartConfigurationPolicyAssociation](#) API desde la cuenta de administrador delegado CSPM de Security Hub en la región de origen.
2. En el campo `ConfigurationPolicyIdentifier`, indique `SELF_MANAGED_SECURITY_HUB` si desea que la cuenta o unidad organizativa controle su propia configuración. Indique el nombre de recurso de Amazon (ARN) o el ID de la

política de configuración correspondiente si desea que el administrador delegado controle la configuración de la cuenta o unidad organizativa.

3. Para el Target campo, proporcione el Cuenta de AWS ID, el ID de la OU o el ID raíz del objetivo cuyo tipo de administración desee cambiar. Esto asocia el comportamiento autoadministrado o la política de configuración especificada al destino. Las cuentas secundarias del destino pueden heredar el comportamiento autoadministrado o la política de configuración.

Ejemplo de solicitud de la API para designar una cuenta autoadministrada:

```
{
  "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
  "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Elección del tipo de administración de una cuenta o unidad organizativa

1. Ejecute el [start-configuration-policy-association](#) comando desde la cuenta de administrador delegado CSPM de Security Hub en la región de origen.
2. En el campo configuration-policy-identifier, indique SELF_MANAGED_SECURITY_HUB si desea que la cuenta o unidad organizativa controle su propia configuración. Indique el nombre de recurso de Amazon (ARN) o el ID de la política de configuración correspondiente si desea que el administrador delegado controle la configuración de la cuenta o unidad organizativa.
3. Para el target campo, proporcione el Cuenta de AWS ID, el ID de la OU o el ID raíz del objetivo cuyo tipo de administración desee cambiar. Esto asocia el comportamiento autoadministrado o la política de configuración especificada al destino. Las cuentas secundarias del destino pueden heredar el comportamiento autoadministrado o la política de configuración.

Ejemplo de comando para designar una cuenta autoadministrada:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
```

```
--target '{"AccountId": "123456789012"}'
```

Cómo funcionan las políticas de configuración en Security Hub (CSPM)

El administrador delegado de AWS Security Hub Cloud Security Posture Management (CSPM) puede crear políticas de configuración para configurar el CSPM del Security Hub, los estándares de seguridad y los controles de seguridad de una organización. Tras crear una política de configuración, el administrador delegado puede asociarla a cuentas, unidades organizativas (OU) específicas o a la raíz. A continuación, la política entra en vigor en las cuentas especificadas o en la raíz. OUs

Para obtener información general sobre las ventajas de la configuración centralizada y su funcionamiento, consulte [Descripción de la configuración central en Security Hub \(CSPM\)](#).

En esta sección, se proporciona información general y detallada de las políticas de configuración.

Consideraciones respecto de la política

Antes de crear una política de configuración en Security Hub CSPM, tenga en cuenta los siguientes detalles.

- Las políticas de configuración deben estar asociadas para que surtan efecto: después de crear una política de configuración, puede asociarla a una o más cuentas, unidades organizativas (OUs) o a la raíz. Una política de configuración se puede asociar a las cuentas, OUs mediante una aplicación directa o mediante la herencia de una unidad organizativa principal.
- Se puede asociar una cuenta o unidad organizativa a una sola política de configuración: para evitar ajustes conflictivos, una cuenta o unidad organizativa solo se puede asociar a una política de configuración en un momento dado. Como alternativa, una cuenta o unidad organizativa puede autoadministrarse.
- Las políticas de configuración están completas: las políticas de configuración proporcionan una especificación completa de la configuración. Por ejemplo, una cuenta secundaria no puede aceptar la configuración de algunos controles de una política ni la configuración de otros controles de otra política. Cuando asocie una política a una cuenta secundaria, asegúrese de que la política especifique toda la configuración que desea que utilice dicha cuenta.
- Las políticas de configuración no se pueden revertir: no existe la opción de revertir una política de configuración después de asociarla a cuentas o OUs. Por ejemplo, si asocias una política de configuración que inhabilita los CloudWatch controles a una cuenta específica y, a continuación, disocias esa política, los CloudWatch controles seguirán deshabilitados en esa cuenta. Para

volver a habilitar CloudWatch los controles, puede asociar la cuenta a una nueva política que habilite los controles. Como alternativa, puede cambiar la cuenta a autogestionada y habilitar cada CloudWatch control de la cuenta.

- Las políticas de configuración entran en vigor en la región de origen y en todas las regiones vinculadas: una política de configuración afecta a todas las cuentas asociadas de la región de origen y a todas las regiones vinculadas. No puede crear una política de configuración que surta efecto solo en algunas de estas regiones y no en otras. La excepción a esto son los [controles que utilizan recursos globales](#). Security Hub (CSPM) deshabilita automáticamente los controles que involucren recursos globales en todas las regiones, excepto en la región de origen.

Las regiones que AWS se introdujeron el 20 de marzo de 2019 o después se denominan regiones de suscripción voluntaria. Debe habilitar dicha región para una cuenta antes de que una política de configuración entre en vigor en ella. La cuenta de administración de Organizations puede habilitar regiones optativas para una cuenta de miembro. Para obtener instrucciones sobre cómo habilitar las regiones opcionales, consulta [Especificar qué regiones puedes usar en Regiones de AWS tu cuenta](#) en la Guía de referencia sobre la administración de AWS cuentas.

Si su política configura un control que no está disponible en la región de origen o en una o más regiones vinculadas, Security Hub CSPM omite la configuración de control en las regiones no disponibles, pero aplica la configuración en las regiones en las que el control está disponible. No posee cobertura para un control que no está disponible en la región de origen ni en ninguna de las regiones vinculadas.

- Las políticas de configuración son recursos: como recurso, una política de configuración tiene un Nombre de recurso de Amazon (ARN) y un identificador único universal (UUID). El ARN del producto tiene el siguiente formato: `arn:partition:securityhub:region:delegated administrator account ID:configuration-policy/configuration policy UUID`. Una configuración autoadministrada no tiene ARN o UUID. El identificador de una configuración autoadministrada es SELF_MANAGED_SECURITY_HUB.

Tipos de políticas de configuración

Cada política de configuración especifica la configuración siguiente:

- Activa o desactiva Security Hub CSPM.
- Habilite uno o más [estándares de seguridad](#).
- Indique qué [controles de seguridad](#) están habilitados en todos los estándares habilitados. Para ello, proporciona una lista de los controles específicos que deben habilitarse, y Security Hub CSPM

deshabilita todos los demás controles, incluidos los nuevos cuando se lanzan. Como alternativa, puede proporcionar una lista de controles específicos que deberían deshabilitarse y Security Hub CSPM habilitará todos los demás controles, incluidos los controles nuevos cuando se publiquen.

- Si lo desea, [personalice parámetros](#) de ciertos controles habilitados en los estándares habilitados.

Las políticas de configuración central no incluyen los ajustes de la AWS Config grabadora. Debe habilitar AWS Config y activar por separado la grabación de los recursos necesarios para que Security Hub CSPM pueda generar hallazgos de control. Para obtener más información, consulte [Consideraciones antes de habilitar y configurar AWS Config](#).

Si usa la configuración central, Security Hub CSPM deshabilita automáticamente los controles que involucran recursos globales en todas las regiones, excepto en la región de origen. Los controles que elija habilitar a través de una política de configuración están habilitados en todas las regiones en las que están disponibles. Para limitar las búsquedas de estos controles a una sola región, puede actualizar la configuración de la AWS Config grabadora y desactivar el registro de recursos globales en todas las regiones, excepto en la región de origen.

Si un control habilitado que implica recursos globales no es compatible en la región de origen, Security Hub CSPM intenta habilitar el control en una región vinculada en la que se admita el control. Con la configuración central, no hay cobertura para un control que no está disponible en la región de origen ni en ninguna de las regiones vinculadas.

Para obtener una lista de los controles que implican recursos globales, consulte [Controles que utilizan recursos globales](#).

Política de configuración recomendada

Al crear una política de configuración por primera vez en la consola CSPM de Security Hub, tiene la opción de elegir la política CSPM recomendada por Security Hub.

La política recomendada habilita el CSPM de Security Hub, el estándar AWS Foundational Security Best Practices (FSBP) y todos los controles FSBP nuevos y existentes. Los controles que aceptan parámetros utilizan los valores predeterminados. La política recomendada se aplica a las cuentas root (todas las cuentas, tanto las nuevas como las existentes). OUs Tras crear la política recomendada para su organización, puede modificarla desde la cuenta de administrador delegado. Por ejemplo, puede habilitar estándares o controles adicionales o deshabilitar controles específicos del FSBP. Para obtener instrucciones sobre cómo modificar una política de configuración, consulte [Actualización de las políticas de configuración](#).

Política de configuración personalizada

En lugar de la política recomendada, el administrador delegado puede crear hasta 20 políticas de configuración personalizadas. Puede asociar una única política personalizada a toda la organización o distintas políticas personalizadas a distintas cuentas y OUs. En el caso de una política de configuración personalizada, debe especificar la configuración que desee. Por ejemplo, puede crear una política personalizada que habilite el FSBP, AWS Foundations Benchmark v1.4.0 de Center for Internet Security (CIS) y todos los controles de esos estándares, excepto los controles de Amazon Redshift. El nivel de granularidad que utilice en las políticas de configuración personalizadas depende del alcance previsto de la cobertura de seguridad en toda la organización.

Note

No puede asociar una política de configuración que deshabilite el CSPM de Security Hub con la cuenta de administrador delegado. Esta política se puede asociar a otras cuentas, pero omite la asociación con el administrador delegado. La cuenta de administrador delegado retiene su configuración actual.

Tras crear una política de configuración personalizada, puede cambiar a la política de configuración recomendada mediante su actualización para que refleje la configuración recomendada. Sin embargo, no verá la opción de crear la política de configuración recomendada en la consola CSPM de Security Hub después de crear la primera política.

Asociación de políticas mediante la aplicación y la herencia

Cuando opta por la configuración centralizada por primera vez, su organización no tiene asociaciones y se comporta de la misma manera que antes de la configuración. A continuación, el administrador delegado puede establecer asociaciones entre una política de configuración o un comportamiento autogestionado y las cuentas o la raíz OUs. Las asociaciones se pueden establecer mediante aplicación o herencia.

Desde la cuenta del administrador delegado, puede aplicar directamente una política de configuración a una cuenta, unidad organizativa o la raíz. Como alternativa, el administrador delegado puede aplicar directamente una designación autoadministrada a una cuenta, unidad organizativa o raíz.

En ausencia de una aplicación directa, una cuenta o unidad organizativa hereda la configuración de la cuenta principal más cercana que tenga una política de configuración o un comportamiento

autoadministrado. Si la cuenta principal más cercana está asociada a una política de configuración, la cuenta secundaria hereda esa política y solo la puede configurar el administrador delegado de la región de origen. Si el padre más cercano es autogestionado, el hijo hereda el comportamiento autogestionado y tiene la capacidad de especificar su propia configuración en cada uno de ellos.

Región de AWS

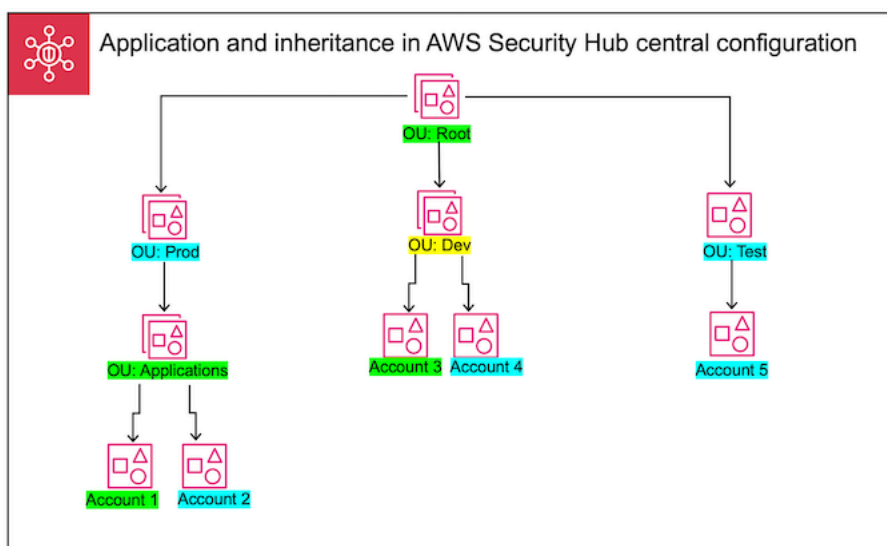
La aplicación tiene prioridad sobre la herencia. En otras palabras, la herencia no anula una política de configuración o una designación autoadministrada que el administrador delegado haya aplicado directamente a una cuenta o unidad organizativa.

Si aplica directamente una política de configuración a una cuenta autoadministrada, la política anula la designación autoadministrada. La cuenta pasa a administrarse de forma centralizada y adopta los ajustes reflejados en la política de configuración.

Recomendamos aplicar directamente una política de configuración a la raíz. Si aplica una política a la raíz, las nuevas cuentas que se unan a su organización heredarán automáticamente la política raíz, a menos que las asocie a una política diferente o las designe como autoadministrables.

Solo se puede asociar una política de configuración a una cuenta o unidad organizativa en un momento dado, ya sea mediante aplicación o herencia. Se diseñó así para evitar configuraciones conflictivas.

El siguiente diagrama ilustra cómo funcionan la aplicación de políticas y la herencia en una configuración centralizada.



En este ejemplo, se ha aplicado una política de configuración a un nodo resaltado en verde. No se ha aplicado ninguna política de configuración al nodo resaltado en azul. Un nodo resaltado en

amarillo se ha designado como autoadministrado. Cada cuenta y unidad organizativa usa la siguiente configuración:

- OU:Root (verde): esta unidad organizativa usa la política de configuración que se le ha aplicado.
- OU:Prod (azul): esta unidad organizativa hereda la política de configuración de OU:Root.
- OU:Applications (verde): esta unidad organizativa usa la política de configuración que se le ha aplicado.
- Cuenta 1 (verde): esta cuenta usa la política de configuración que se le ha aplicado.
- Cuenta 2 (azul): esta cuenta hereda la política de configuración de OU:Applications.
- OU:Dev (amarillo): esta unidad organizativa está autoadministrada.
- Cuenta 3 (verde): esta cuenta usa la política de configuración que se le ha aplicado.
- Cuenta 4 (azul): esta cuenta hereda el comportamiento autoadministrado de OU:Dev.
- OU:Test (Blue): esta cuenta hereda la política de configuración de OU:Root.
- Cuenta 5 (azul): esta cuenta hereda la política de configuración de OU:Root, ya que su matriz inmediata, OU:Test, no está asociada a ninguna política de configuración.

Prueba de una política de configuración

Para asegurarse de que comprende cómo funcionan las políticas de configuración, le recomendamos crear una política y asociarla a una cuenta de prueba o unidad organizativa.

Prueba de una política de configuración

1. Cree una política de configuración personalizada y compruebe que los ajustes especificados para la habilitación, los estándares y los controles del CSPM de Security Hub sean correctos. Para obtener instrucciones, consulte [Creación y asociación de políticas de configuración](#).
2. Aplique la política de configuración a una cuenta de prueba o unidad organizativa que no tenga ninguna cuenta secundaria o. OUs
3. Compruebe que la cuenta de prueba o la unidad organizativa utilicen la política de configuración de la manera esperada en su región de origen y en todas las regiones vinculadas. También puede comprobar que todas las demás cuentas de su organización siguen siendo autogestionadas y pueden cambiar sus propios ajustes en cada región. OUs

Después de probar una política de configuración en una sola cuenta o unidad organizativa, puede asociarla a otras cuentas y OUs.

Creación y asociación de políticas de configuración

La cuenta de administrador delegada de AWS Security Hub Cloud Security Posture Management (CSPM) puede crear políticas de configuración que especifiquen cómo se configuran el CSPM, los estándares y los controles de Security Hub en cuentas y unidades organizativas específicas (). OUs Una política de configuración solo entra en vigor después de que el administrador delegado la asocie al menos a una cuenta o unidad organizativa () OUs o a la raíz. El administrador delegado también puede asociar una configuración autogestionada a las cuentas o a la OUs raíz.

Si es la primera vez que crea una política de configuración, le recomienda que revise antes [Cómo funcionan las políticas de configuración en Security Hub \(CSPM\)](#).

Elija el método de acceso que prefiera y siga los pasos para crear y asociar una política de configuración o una configuración autoadministrada. Al utilizar la consola CSPM de Security Hub, puede asociar una configuración a varias cuentas o OUs al mismo tiempo. Al utilizar la API CSPM de Security Hub o AWS CLI, puede asociar una configuración a una sola cuenta o unidad organizativa en cada solicitud.

Note

Si usa la configuración central, Security Hub CSPM deshabilita automáticamente los controles que involucran recursos globales en todas las regiones, excepto en la región de origen. Los controles que elija habilitar a través de una política de configuración están habilitados en todas las regiones en las que están disponibles. Para limitar las búsquedas de estos controles a una sola región, puede actualizar la configuración de la AWS Config grabadora y desactivar el registro de recursos globales en todas las regiones, excepto en la región de origen.

Si un control habilitado que implica recursos globales no es compatible en la región de origen, Security Hub CSPM intenta habilitar el control en una región vinculada en la que se admita el control. Con la configuración central, no hay cobertura para un control que no está disponible en la región de origen ni en ninguna de las regiones vinculadas.

Para obtener una lista de los controles que implican recursos globales, consulte [Controles que utilizan recursos globales](#).

Security Hub CSPM console

Creación y asociación de políticas de configuración

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en.
<https://console.aws.amazon.com/securityhub/>

Inicie sesión con las credenciales de la cuenta de administrador CSPM de Security Hub delegada en la región de origen.

2. En el panel de navegación, seleccione Configuración y la pestaña Políticas. A continuación, seleccione Crear política.
3. En la página Configurar organización, si es la primera vez que crea una política de configuración, verá tres opciones en Tipo de configuración. Si ya ha creado al menos una política de configuración, solo verá la opción Política personalizada.
 - Elija Usar la configuración CSPM de Security Hub AWS recomendada en toda mi organización para usar nuestra política recomendada. La política recomendada habilita el CSPM de Security Hub en todas las cuentas de la organización, habilita el estándar AWS Foundational Security Best Practices (FSBP) y habilita todos los controles FSBP nuevos y existentes. Los controles utilizan valores de parámetros predeterminados.
 - Para crear una política de configuración más tarde, seleccione Aún no lo tengo todo listo para configurarla.
 - Seleccione Política personalizada para crear una política de configuración personalizada. Especifique si desea habilitar o deshabilitar el CSPM de Security Hub, qué estándares habilitar y qué controles habilitar en todos esos estándares. Si lo desea, especifique [valores de parámetros personalizados](#) para uno o más controles habilitados que admitan parámetros personalizados.
4. En la sección Cuentas, elija las cuentas de destino o las cuentas raíz a las que desea que se aplique la política de configuración. OUs
 - Seleccione Todas las cuentas si desea aplicar la política de configuración a la raíz. Esto incluye todas las cuentas de OUs la organización a las que no se les haya aplicado o heredado otra política.
 - Elija Cuentas específicas si desea aplicar la política de configuración a cuentas específicas o OUs. Introduzca la cuenta IDs o seleccione las cuentas y la estructura OUs de la organización. Puede aplicar la política a un máximo de 15 objetivos (cuentas o root) al

crearla. OUs Para especificar un número mayor, edite la política después de crearla y aplíquela a destinos adicionales.

- Seleccione Solo el administrador delegado para aplicar la política de configuración a la cuenta de administrador delegado actual.

5. Elija Siguiente.

6. En la página Revisar y aplicar, revise los detalles de la política de configuración. A continuación, seleccione Crear y aplicar política. Tanto en su región de origen como en las regiones vinculadas, esta acción anula los ajustes de configuración existentes de las cuentas asociadas a esta política de configuración. Las cuentas se pueden asociar a la política de configuración mediante una aplicación o la herencia de un nodo principal. Las cuentas secundarias y OUs los destinos aplicados heredarán automáticamente esta política de configuración, a menos que se excluyan específicamente, se autoadministren o utilicen una política de configuración diferente.

Security Hub CSPM API

Creación y asociación de políticas de configuración

1. Invoque la [CreateConfigurationPolicy](#) API desde la cuenta de administrador delegado CSPM de Security Hub en la región de origen.
2. En Name, especifique un nombre para la política de configuración. Si lo desea, en el caso de Description, proporcione una descripción de la política de configuración.
3. Para el ServiceEnabled campo, especifique si desea que Security Hub CSPM esté habilitado o deshabilitado en esta política de configuración.
4. Para el EnabledStandardIdentifiers campo, especifique qué estándares CSPM de Security Hub quiere habilitar en esta política de configuración.
5. Para el objeto SecurityControlsConfiguration, especifique qué controles desea habilitar o deshabilitar en esta política de configuración. Elegir EnabledSecurityControlIdentifiers significa que los controles especificados están habilitados. Otros controles que forman parte de los estándares habilitados (como los controles recién lanzados) están deshabilitados. Elegir DisabledSecurityControlIdentifiers significa que los controles especificados están deshabilitados. Otros controles que forman parte de los estándares habilitados (como los controles recién lanzados) están habilitados.

6. Si lo desea, en el campo `SecurityControlCustomParameters`, especifique los controles habilitados para los que desee personalizar los parámetros. Indique `CUSTOM` en el campo `ValueType` y el valor del parámetro personalizado para el campo `Value`. El valor debe ser del tipo de datos correcto y estar dentro de los rangos válidos especificados por Security Hub CSPM. Solo algunos controles admiten valores de parámetros personalizados. Para obtener más información, consulte [Descripción de los parámetros de control en Security Hub CSPM](#).
7. Para aplicar su política de configuración a las cuentas o OUs, invoque la [StartConfigurationPolicyAssociation](#) API desde la cuenta de administrador delegado CSPM de Security Hub en la región de origen.
8. En el campo `ConfigurationPolicyIdentifier`, indique el nombre de recurso de Amazon (ARN) o el identificador único universal (UUID) de la política. La API `CreateConfigurationPolicy` devuelve el ARN y el UUID. En una configuración autoadministrada, el campo `ConfigurationPolicyIdentifier` es igual a `SELF_MANAGED_SECURITY_HUB`.
9. En el campo `Target`, indique el ID de raíz, unidad organizativa, o cuenta donde desea que se aplique esta política de configuración. Solo puede proporcionar un objetivo en cada solicitud de API. Las cuentas secundarias y OUs del destino seleccionado heredarán automáticamente esta política de configuración, a menos que se autoadministren o utilicen una política de configuración diferente.

Ejemplo de solicitud de API para crear una política de configuración:

```
{
  "Name": "SampleConfigurationPolicy",
  "Description": "Configuration policy for production accounts",
  "ConfigurationPolicy": {
    "SecurityHub": {
      "ServiceEnabled": true,
      "EnabledStandardIdentifiers": [
        "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
        "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
      ],
      "SecurityControlsConfiguration": {
        "DisabledSecurityControlIdentifiers": [
          "CloudTrail.2"
        ]
      }
    }
  }
}
```

```

    "SecurityControlCustomParameters": [
      {
        "SecurityControlId": "ACM.1",
        "Parameters": {
          "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
              "Integer": 15
            }
          }
        }
      }
    ]
  }
}

```

Ejemplo de solicitud de API para asociar una política de configuración:

```

{
  "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}

```

AWS CLI

Creación y asociación de políticas de configuración

1. Ejecute el [create-configuration-policy](#) comando desde la cuenta de administrador delegado CSPM de Security Hub en la región de origen.
2. En name, especifique un nombre para la política de configuración. Si lo desea, en el caso de description, proporcione una descripción de la política de configuración.
3. Para el ServiceEnabled campo, especifique si desea que Security Hub CSPM esté habilitado o deshabilitado en esta política de configuración.
4. Para el EnabledStandardIdentifiers campo, especifique qué estándares CSPM de Security Hub quiere habilitar en esta política de configuración.

5. En el campo `SecurityControlsConfiguration`, especifique qué controles desea habilitar o deshabilitar en esta política de configuración. Elegir `EnabledSecurityControlIdentifiers` significa que los controles especificados están habilitados. Otros controles que forman parte de los estándares habilitados (como los controles recién lanzados) están deshabilitados. Elegir `DisabledSecurityControlIdentifiers` significa que los controles especificados están deshabilitados. Se han habilitado otros controles que se aplican a los estándares habilitados (como los controles recién lanzados).
6. Si lo desea, en el campo `SecurityControlCustomParameters`, especifique los controles habilitados para los que desee personalizar los parámetros. Indique `CUSTOM` en el campo `ValueType` y el valor del parámetro personalizado para el campo `Value`. El valor debe ser del tipo de datos correcto y estar dentro de los rangos válidos especificados por Security Hub CSPM. Solo algunos controles admiten valores de parámetros personalizados. Para obtener más información, consulte [Descripción de los parámetros de control en Security Hub CSPM](#).
7. Para aplicar la política de configuración a las cuentas o OUs, ejecute el [start-configuration-policy-association](#) comando desde la cuenta de administrador delegado CSPM de Security Hub en la región de origen.
8. En el campo `configuration-policy-identifier`, indique el nombre de recurso de Amazon (ARN) o el ID de la política de configuración. El comando `create-configuration-policy` devuelve este ARN e ID.
9. En el campo `target`, indique el ID de raíz, unidad organizativa, o cuenta donde desea que se aplique esta política de configuración. Solo puede proporcionar un destino cada vez que ejecute el comando. Las entidades secundarias de los destinos seleccionados heredarán automáticamente esta política de configuración, a menos que se autoadministren o utilicen una política de configuración diferente.

Ejemplo de comando para crear una política de configuración:

```
aws securityhub --region us-east-1 create-configuration-policy \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
"EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "arn:aws:securityhub::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"], "SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"]},
```

```
"SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters": [{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}]}]}
```

Ejemplo de comando para asociar una política de configuración:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}'
```

La API `StartConfigurationPolicyAssociation` devuelve un campo llamado `AssociationStatus`. Este campo indica si la asociación de una política está pendiente o si su estado es correcto o incorrecto. El estado puede tardar hasta 24 horas minutos en cambiar de `PENDING` a `SUCCESS` o `FAILURE`. Para obtener más información sobre el estado de una asociación, consulte [Revisión del estado de asociación de una política de configuración](#).

Revisión del estado y los detalles de las políticas de configuración

El administrador delegado de AWS Security Hub Cloud Security Posture Management (CSPM) puede ver las políticas de configuración de una organización y sus detalles. Esto incluye las cuentas y unidades organizativas (OUs) a las que está asociada una política.

Para obtener información general sobre las ventajas de la configuración centralizada y su funcionamiento, consulte [Descripción de la configuración central en Security Hub \(CSPM\)](#).

Elija su método preferido y siga estos pasos para ver las políticas de configuración.

Security Hub CSPM console

Para ver políticas de configuración (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
Inicie sesión con las credenciales de la cuenta de administrador CSPM de Security Hub delegada en la región de origen.
2. En el panel de navegación, seleccione Configuración y Configuración.
3. Seleccione la pestaña Políticas para obtener un resumen de las políticas de configuración.

4. Seleccione una política de configuración y elija Ver detalles para ver detalles adicionales sobre ella, incluidas las cuentas a las que OUs está asociada.

Security Hub CSPM API

Para ver una lista resumida de todas sus políticas de configuración, utilice el [ListConfigurationPolicies](#) funcionamiento de la API CSPM de Security Hub. Si usa el AWS CLI, ejecute el [list-configuration-policies](#) comando. La cuenta de administrador de CSPM de Security Hub delegada debe invocar la operación en la región de origen.

```
$ aws securityhub list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutLYJHWpn9xnG4hqS0hvw3o2JqjI23QDxdf
```

Para ver los detalles sobre una política de configuración específica, utilice la operación [GetConfigurationPolicy](#). Si usa el, ejecute el AWS CLI. [get-configuration-policy](#) La cuenta de administrador delegado debe invocar la operación en la región de origen. Proporcione el nombre de recurso de Amazon (ARN) o el ID de la política de configuración cuyos detalles desea ver.

```
$ aws securityhub get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE1111"
```

Para ver una lista resumida de todas las políticas de configuración y sus respectivas asociaciones de cuentas, utilice la operación de configuración [ListConfigurationPolicyAssociations](#). Si usa el AWS CLI, ejecute el [list-configuration-policy-associations](#) comando. La cuenta de administrador delegado debe invocar la operación en la región de origen. Si lo desea, puede proporcionar parámetros de paginación o filtrar los resultados por un ID de política, un tipo de asociación o un estado de asociación específico.

```
$ aws securityhub list-configuration-policy-associations \
--filters '{"AssociationType": "APPLIED"}'
```

Para ver las asociaciones de una cuenta específica, utilice la operación [GetConfigurationPolicyAssociation](#). Si usa el AWS CLI, ejecute el [get-configuration-policy-association](#) comando. La cuenta de administrador delegado debe invocar la operación en la región de origen. En target, indique el número de cuenta, el ID de unidad organizativa o el ID de raíz.

```
$ aws securityhub get-configuration-policy-association \
```

```
--target '{"AccountId": "123456789012"}'
```

Revisión del estado de asociación de una política de configuración

Las siguientes operaciones de la API de configuración centralizada devuelven un campo denominado `AssociationStatus`:

- `BatchGetConfigurationPolicyAssociations`
- `GetConfigurationPolicyAssociation`
- `ListConfigurationPolicyAssociations`
- `StartConfigurationPolicyAssociation`

Este campo se devuelve cuando la configuración subyacente es una política de configuración y cuando se trata de un comportamiento autoadministrado.

El valor de `AssociationStatus` indica si una asociación de políticas está pendiente o se encuentra en un estado de éxito o fracaso para una cuenta específica. El estado puede tardar hasta 24 horas minutos en cambiar de `PENDING` a `SUCCESS` o `FAILED`. Un estado de `SUCCESS` significa que todos los ajustes especificados en la política de configuración están asociados a la cuenta. Un estado de `FAILED` significa que una o más opciones especificadas en la política de configuración no se pudieron asociar a la cuenta. A pesar `FAILED` del estado, la cuenta podría configurarse parcialmente de acuerdo con la política. Por ejemplo, puede intentar asociar una cuenta a una política de configuración que habilite el CSPM de Security Hub, habilite las prácticas recomendadas de seguridad AWS fundamentales y deshabilite .1. CloudTrail Las dos configuraciones iniciales podrían funcionar correctamente, pero la configuración CloudTrail .1 podría fallar. En este ejemplo, el estado de la asociación es igual a `FAILED` pesar de que algunos ajustes se configuraron correctamente.

El estado de asociación de una unidad organizativa principal o de la raíz depende del estado de sus entidades secundarias. Si el estado de asociación de todas las entidades secundarias es `SUCCESS`, el estado de asociación de la entidad principal es `SUCCESS`. Si el estado de asociación de una o más entidades secundarias es `FAILED`, el estado de asociación de la entidad principal es `FAILED`.

El valor de `AssociationStatus` depende del estado de asociación de la política en todas las regiones pertinentes. Si la asociación tiene éxito en la región de origen y en todas las regiones vinculadas, el valor de `AssociationStatus` es `SUCCESS`. Si se produce un error en la asociación en una o más de estas regiones, el valor de `AssociationStatus` es `FAILED`.

El siguiente comportamiento también afecta al valor de `AssociationStatus`:

- Si el destino es una unidad organizativa principal o de la raíz, tiene un `AssociationStatus` de `SUCCESS` o `FAILED` solo cuando todas las entidades secundarias tienen un estado `SUCCESS` o `FAILED`. Si el estado de asociación de una cuenta o unidad organizativa secundaria cambia (por ejemplo, cuando se agrega o elimina una región vinculada) después de asociar por primera vez la entidad principal a una configuración, el cambio no actualiza el estado de asociación de la entidad principal a menos que vuelva a invocar la API `StartConfigurationPolicyAssociation`.
- Si el destino es una cuenta, tiene un `AssociationStatus` de `SUCCESS` o `FAILED` solo si la asociación tiene un resultado de `SUCCESS` o `FAILED` en la región de origen y en todas las regiones vinculadas. Si el estado de asociación de una cuenta de destino cambia (por ejemplo, cuando se agrega o elimina una región vinculada) después de asociarla por primera vez a una configuración, su estado de asociación se actualiza. Sin embargo, el cambio no actualiza el estado de asociación de la entidad principal a menos que vuelva a invocar la API `StartConfigurationPolicyAssociation`.

Si agrega una nueva región vinculada, Security Hub CSPM replica las asociaciones existentes que se encuentran en una o en un `PENDING` `FAILED` estado de la nueva región. `SUCCESS`

Incluso si el estado de la asociación es el `SUCCESS` mismo, el estado de habilitación de un estándar que forma parte de la política puede pasar a un estado incompleto. En ese caso, Security Hub CSPM no puede generar resultados para los controles del estándar. Para obtener más información, consulte [Comprobar el estado de un estándar](#).

Solución de problemas de la asociación

En AWS Security Hub Cloud Security Posture Management (CSPM), la asociación de una política de configuración puede fallar por los siguientes motivos habituales.

- La cuenta de administración de Organizations no es miembro: si quieres asociar una política de configuración a la cuenta de administración de Organizations, esa cuenta ya debe tener AWS habilitada la Administración de Postura de Seguridad (CSPM) de Security Hub Cloud. Esto convierte a la cuenta de administración en una cuenta de miembro de la organización.
- AWS Config no está habilitada o configurada correctamente: para habilitar los estándares en una política de configuración, AWS Config debe estar habilitada y configurada para registrar los recursos relevantes.

- Debe asociarse desde una cuenta de administrador delegada: solo puede asociar una política a las cuentas de destino y OUs cuando haya iniciado sesión en la cuenta de administrador delegada de CSPM de Security Hub.
- Debe asociarse desde la región de origen: solo puede asociar una política a las cuentas de destino y OUs cuando haya iniciado sesión en su región de origen.
- La región optativa no está habilitada: no se puede asociar la política a una cuenta de miembro o unidad organizativa de una región vinculada si se trata de una región optativa que el administrador delegado no ha habilitado. Puede volver a intentarlo después de habilitar la región desde la cuenta de administrador delegado.
- Cuenta de miembro suspendida: la asociación de políticas es muestra error si se intenta asociar una política a una cuenta de miembro suspendida.

Actualización de las políticas de configuración

Tras crear una política de configuración, la cuenta de administrador delegada de AWS Security Hub Cloud Security Posture Management (CSPM) puede actualizar los detalles de la política y las asociaciones de políticas. Cuando se actualizan los detalles de la política, las cuentas asociadas a la política de configuración comienzan a utilizar de manera automática la política actualizada.

Para obtener información general sobre las ventajas de la configuración centralizada y su funcionamiento, consulte [Descripción de la configuración central en Security Hub \(CSPM\)](#).

El administrador delegado puede actualizar los siguientes ajustes de la política:

- Activa o desactiva Security Hub CSPM.
- Habilite uno o más [estándares de seguridad](#).
- Indique qué [controles de seguridad](#) están habilitados en todos los estándares habilitados. Para ello, puede proporcionar una lista de controles específicos que deberían estar habilitados, y Security Hub CSPM deshabilita todos los demás controles, incluidos los nuevos cuando se lanzan. Como alternativa, puede proporcionar una lista de controles específicos que deberían deshabilitarse y Security Hub CSPM habilitará todos los demás controles, incluidos los controles nuevos cuando se publiquen.
- Si lo desea, [personalice parámetros](#) de ciertos controles habilitados en los estándares habilitados.

Elija su método preferido y siga estos pasos para actualizar una política de configuración.

 Note

Si usa la configuración central, Security Hub CSPM deshabilita automáticamente los controles que involucren recursos globales en todas las regiones, excepto en la región de origen. Los controles que elija habilitar a través de una política de configuración están habilitados en todas las regiones en las que están disponibles. Para limitar las búsquedas de estos controles a una sola región, puede actualizar la configuración de la AWS Config grabadora y desactivar el registro de recursos globales en todas las regiones, excepto en la región de origen.

Si un control habilitado que implica recursos globales no es compatible en la región de origen, Security Hub CSPM intenta habilitar el control en una región vinculada en la que se admita el control. Con la configuración central, no hay cobertura para un control que no está disponible en la región de origen ni en ninguna de las regiones vinculadas.

Para obtener una lista de los controles que implican recursos globales, consulte [Controles que utilizan recursos globales](#).

Console

Actualización de las políticas de configuración

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>

Inicie sesión con las credenciales de la cuenta de administrador CSPM de Security Hub delegada en la región de origen.
2. En el panel de navegación, seleccione Configuración y Configuración.
3. Elija la pestaña Políticas.
4. Seleccione la política de configuración que desea modificar y elija Editar. Si lo desea, edite la configuración de la política. Deje esta sección como está si desea mantener la configuración de la política sin cambios.
5. Seleccione Siguiente. Si lo desea, edite las asociaciones de políticas. Deje esta sección como está si desea mantener las asociaciones de políticas sin cambios. Puede asociar o desasociar la política a un máximo de 15 destinos (cuentas o root) al actualizarla. OUs
6. Elija Siguiente.

7. Revise los cambios y seleccione Guardar y aplicar. Tanto en su región de origen como en las regiones vinculadas, esta acción anula los ajustes de configuración existentes de las cuentas asociadas a esta política de configuración. Las cuentas se pueden asociar a una política de configuración mediante una aplicación o la herencia de un nodo principal.

API

Actualización de las políticas de configuración

1. Para actualizar los ajustes de una política de configuración, invoque la [UpdateConfigurationPolicy](#) API desde la cuenta de administrador delegado CSPM de Security Hub en la región de origen.
2. Proporcione el nombre de recurso de Amazon (ARN) o el ID de la política de configuración que desea actualizar.
3. Proporcione valores actualizados para los campos de ConfigurationPolicy. También tiene la opción de indicar el motivo de la actualización.
4. Para añadir nuevas asociaciones para esta política de configuración, invoque la [StartConfigurationPolicyAssociation](#) API desde la cuenta de administrador delegado CSPM de Security Hub en la región de origen. Para eliminar una o más asociaciones actuales, invoque la [StartConfigurationPolicyDisassociation](#) API desde la cuenta de administrador delegado CSPM de Security Hub en la región de origen.
5. En el campo ConfigurationPolicyIdentifier, indique el ARN o el ID de la política de configuración cuyas asociaciones desee actualizar.
6. Para el Target campo, proporcione las cuentas o el ID raíz que desee asociar o desasociar. OUs Esta acción anula las asociaciones de políticas anteriores para las cuentas OUs o cuentas especificadas.

Note

Al invocar la UpdateConfigurationPolicy API, Security Hub CSPM sustituye por una lista completa los campos EnabledStandardIdentifiers, EnabledSecurityControlIdentifiersDisabledSecurityControlIdentifiers, y SecurityControlCustomParameters Cada vez que invoque esta API, proporcione la lista completa de estándares que desee habilitar y la lista completa de controles que desee habilitar o deshabilitar y para los que desee personalizar los parámetros.

Ejemplo de solicitud de API para actualizar una política de configuración:

```
{
  "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Description": "Updated configuration policy",
  "UpdatedReason": "Disabling CloudWatch.1",
  "ConfigurationPolicy": {
    "SecurityHub": {
      "ServiceEnabled": true,
      "EnabledStandardIdentifiers": [
        "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
        "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
      ],
      "SecurityControlsConfiguration": {
        "DisabledSecurityControlIdentifiers": [
          "CloudTrail.2",
          "CloudWatch.1"
        ],
        "SecurityControlCustomParameters": [
          {
            "SecurityControlId": "ACM.1",
            "Parameters": {
              "daysToExpiration": {
                "ValueType": "CUSTOM",
                "Value": {
                  "Integer": 15
                }
              }
            }
          }
        ]
      }
    }
  }
}
```

AWS CLI

Actualización de las políticas de configuración

1. Para actualizar los ajustes de una política de configuración, ejecute el [update-configuration-policy](#) comando desde la cuenta de administrador delegado CSPM de Security Hub en la región de origen.
2. Proporcione el nombre de recurso de Amazon (ARN) o el ID de la política de configuración que desea actualizar.
3. Proporcione valores actualizados para los campos de configuration-policy. También tiene la opción de indicar el motivo de la actualización.
4. Para añadir nuevas asociaciones para esta política de configuración, ejecute el [start-configuration-policy-association](#) comando desde la cuenta de administrador delegado CSPM de Security Hub en la región de origen. Para eliminar una o más asociaciones actuales, ejecute el [start-configuration-policy-disassociation](#) comando desde la cuenta de administrador delegado CSPM de Security Hub en la región de origen.
5. En el campo configuration-policy-identifier, indique el ARN o el ID de la política de configuración cuyas asociaciones desee actualizar.
6. Para el target campo, proporcione las cuentas o el ID raíz que desee asociar o desasociar. OUs Esta acción anula las asociaciones de políticas anteriores para las cuentas OUs o cuentas especificadas.

Note

Al ejecutar el update-configuration-policy comando, Security Hub CSPM reemplaza la lista completa de los campos EnabledStandardIdentifiers, EnabledSecurityControlIdentifiersDisabledSecurityControlIdentifiers, y SecurityControlCustomParameters. Cada vez que ejecute este comando, proporcione la lista completa de estándares que desee habilitar y la lista completa de controles que desee habilitar o deshabilitar y para los que desee personalizar los parámetros.

Ejemplo de comando para actualizar una política de configuración:

```
aws securityhub update-configuration-policy \
```



```
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--description "Updated configuration policy" \
--updated-reason "Disabling CloudWatch.1" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
"EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "arn:aws:securityhub::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"], "SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2", "CloudWatch.1"],
"SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}]}}}'
```

La API `StartConfigurationPolicyAssociation` devuelve un campo llamado `AssociationStatus`. Este campo indica si la asociación de una política está pendiente o si su estado es correcto o incorrecto. El estado puede tardar hasta 24 horas minutos en cambiar de `PENDING` a `SUCCESS` o `FAILURE`. Para obtener más información sobre el estado de una asociación, consulte [Revisión del estado de asociación de una política de configuración](#).

Eliminación de políticas de configuración

Tras crear una política de configuración, el administrador delegado de AWS Security Hub Cloud Security Posture Management (CSPM) puede eliminarla. Como alternativa, el administrador delegado puede conservar la política, pero disociarla de cuentas o unidades organizativas específicas (OUs) o de la raíz. Para obtener instrucciones sobre cómo desasociar una política, consulte [Desasociación de una configuración de sus objetivos](#).

Para obtener información general sobre las ventajas de la configuración centralizada y su funcionamiento, consulte [Descripción de la configuración central en Security Hub \(CSPM\)](#).

En esta sección se explica cómo eliminar políticas de configuración.

Al eliminar una política de configuración, esta deja de existir en su organización. Las cuentas de destino y la raíz de la organización ya no pueden usar la política de configuración. OUs Los destinos que estaban asociados a una política de configuración eliminada heredan la política de configuración de la entidad principal más próxima o se vuelven autoadministrados si la entidad principal más próxima se autoadministra. Si desea que un destino utilice una configuración diferente, puede asociar el destino a una nueva política de configuración. Para obtener más información, consulte [Creación y asociación de políticas de configuración](#).

Se recomienda crear y asociar al menos una política de configuración a su organización para proporcionar una cobertura de seguridad adecuada.

Para poder eliminar una política de configuración, debe desasociarla de cualquier cuenta o raíz a la que se aplique actualmente. OUs

Elija su método preferido y siga estos pasos para eliminar una política de configuración.

Console

Eliminación de una política de configuración

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>

Inicie sesión con las credenciales de la cuenta de administrador CSPM de Security Hub delegada en la región de origen.
2. En el panel de navegación, seleccione Configuración y Configuración.
3. Elija la pestaña Políticas. Seleccione la política de configuración que desea eliminar y, a continuación, elija Eliminar. Si la política de configuración sigue asociada a alguna cuenta o OUs, se le pedirá que primero desasocie la política de esos destinos antes de poder eliminarla.
4. Revise el mensaje de confirmación. Ingrese **confirm** y elija Eliminar.

API

Eliminación de una política de configuración

Invoque la [DeleteConfigurationPolicy](#) API desde la cuenta de administrador delegado CSPM de Security Hub en la región de origen.

Proporcione el nombre de recurso de Amazon (ARN) o el ID de la política de configuración que desea eliminar. Si recibe un `ConflictException` error, la política de configuración seguirá aplicándose a las cuentas o OUs a su organización. Para resolver el error, desasocie la política de configuración de estas cuentas o OUs antes de intentar eliminarla.

Ejemplo de solicitud de API para eliminar una política de configuración:

```
{
```

```
"Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

Eliminación de una política de configuración

Ejecute el [delete-configuration-policy](#) comando desde la cuenta de administrador delegado CSPM de Security Hub en la región de origen.

Proporcione el nombre de recurso de Amazon (ARN) o el ID de la política de configuración que desea eliminar. Si recibe un `ConflictException` error, la política de configuración seguirá aplicándose a las cuentas o OUs a su organización. Para resolver el error, desasocie la política de configuración de estas cuentas o OUs antes de intentar eliminarla.

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Desasociación de una configuración de sus objetivos

Desde la cuenta de administrador delegada de AWS Security Hub Cloud Security Posture Management (CSPM), puede desasociar una política de configuración o una configuración autogestionada de una cuenta, unidad organizativa o raíz. La desasociación conserva la política para su uso futuro, pero elimina las asociaciones existentes de cuentas específicas o de la raíz. Solo puede desasociar una configuración aplicada directamente, no una configuración heredada. OUs Para cambiar una configuración heredada, puede aplicar una política de configuración o un comportamiento autoadministrado a la cuenta o unidad organizativa afectada. También puede aplicar una nueva política de configuración, que incluya las modificaciones que desee, a la entidad principal más próxima.

La desasociación no elimina una política de configuración. La política se retiene en su cuenta, por lo que puede asociarla a otros destinos de su organización. Para obtener instrucciones sobre cómo eliminar una política de configuración, consulte [Eliminación de políticas de configuración](#). Cuando se completa la desasociación, el destino afectado hereda la política de configuración o el comportamiento autoadministrado de la entidad principal más próxima. Si no hay una configuración

heredable, el destino conserva la configuración que tenía antes de la desasociación, pero pasa a ser autoadministrado.

Elija el método que prefiera y siga los pasos para desasociar una cuenta, unidad organizativa o raíz de su configuración actual.

Console

Desasociación de una cuenta o unidad organizativa de su configuración actual

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>.

Inicie sesión con las credenciales de la cuenta de administrador CSPM de Security Hub delegada en la región de origen.
2. En el panel de navegación, seleccione Configuración y Configuración.
3. En la pestaña Organizaciones, seleccione la cuenta, unidad organizativa o la raíz que desee desasociar de su configuración actual. Seleccione Editar.
4. En la página Definir configuración, en Administración, elija Política aplicada si desea que el administrador delegado tenga autorización para aplicar las políticas directamente al destino. Elija Heredada si desea que el destino herede la configuración de su entidad principal más próxima. En cualquiera de estos casos, el administrador delegado controla la configuración del destino. Elija Autoadministrada si desea que la cuenta o la unidad organizativa controlen su propia configuración.
5. Tras revisar los cambios, seleccione Siguiente y Aplicar. Esta acción anula las configuraciones existentes de cualquier cuenta o OUs que esté dentro del ámbito de aplicación, si esas configuraciones entran en conflicto con sus selecciones actuales.

API

Desasociación de una cuenta o unidad organizativa de su configuración actual

1. Invoque la [StartConfigurationPolicyDisassociation](#) API desde la cuenta de administrador delegado CSPM de Security Hub en la región de origen.
2. En ConfigurationPolicyIdentifier, indique el nombre de recurso de Amazon (ARN) o el ID de la política de configuración que desee desasociar. Indique SELF_MANAGED_SECURITY_HUB en este campo para desasociar el comportamiento autoadministrado.

3. Para Target ello, indique las cuentas o la raíz que desee disociar de esta política de configuración. OUs

Ejemplo de solicitud de API para desasociar una política de configuración:

```
{
  "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

Desasociación de una cuenta o unidad organizativa de su configuración actual

1. Ejecute el [start-configuration-policy-disassociation](#) comando desde la cuenta de administrador delegado CSPM de Security Hub en la región de origen.
2. En configuration-policy-identifier, indique el nombre de recurso de Amazon (ARN) o el ID de la política de configuración que desee desasociar. Indique SELF_MANAGED_SECURITY_HUB en este campo para desasociar el comportamiento autoadministrado.
3. Para target ello, indique las cuentas o la raíz que desee disociar de esta política de configuración. OUs

Ejemplo de comando para desasociar una política de configuración:

```
aws securityhub --region us-east-1 start-configuration-policy-disassociation \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"RootId": "r-f6g7h8i9j0example"}'
```

Configuración de un estándar o control en su contexto

Al utilizar la [configuración central](#) en AWS Security Hub Cloud Security Posture Management (CSPM), el administrador delegado del Security Hub CSPM puede crear políticas de configuración

que especifiquen cómo se configuran el CSPM, los estándares de seguridad y los controles de seguridad de Security Hub para una organización. El administrador delegado puede asociar políticas a cuentas y unidades organizativas (OU) específicas. Las políticas entran en vigor en su región de origen y en todas las regiones vinculadas. El administrador delegado puede actualizar las políticas de configuración según sea necesario.

En la consola CSPM de Security Hub, el administrador delegado puede actualizar las políticas de configuración de dos maneras: desde la página de configuración o en el contexto de los flujos de trabajo existentes. Esto último puede resultar beneficioso porque, a medida que analiza los resultados de seguridad, puede descubrir qué estándares y controles son más relevantes para su entorno y configurarlos al mismo tiempo.

La configuración contextual solo está disponible en la consola CSPM de Security Hub. De forma programática, el administrador delegado debe invocar el [UpdateConfigurationPolicy](#) funcionamiento de la API CSPM de Security Hub para cambiar la forma en que se configuran los estándares o controles específicos en la organización.

Siga estos pasos para configurar un estándar o control CSPM de Security Hub en su contexto.

Para configurar un estándar o un control en su contexto (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>

Inicie sesión con las credenciales de la cuenta de administrador CSPM de Security Hub delegada en la región de origen.
2. En el panel de navegación, elija una de las siguientes opciones:
 - Para configurar un estándar, elija Estándares de seguridad y elija un estándar específico.
 - Para configurar un control, elija Controles y elija un control específico.
3. La consola muestra las políticas de configuración de CSPM de Security Hub existentes y el estado del estándar o control seleccionado en cada una de ellas. Elija las opciones para habilitar o deshabilitar el estándar o el control en cada política de configuración existente. En el caso de los controles, también puede optar por personalizar [los parámetros de control](#). No puede crear una política nueva durante la configuración en contexto. Para crear una nueva política, debe ir a la página Configuración, elegir la pestaña Políticas y, a continuación, elegir Crear política.
4. Cuando termine de aplicar los cambios, seleccione Siguiente.

5. Revise los cambios y elija Aplicar. Las actualizaciones afectan a todas las cuentas OUs que estén asociadas a una política de configuración modificada. Las actualizaciones también se aplican a la región de origen y a todas las regiones vinculadas.

Desactivación de la configuración central en Security Hub (CSPM)

Al deshabilitar la configuración central en AWS Security Hub Cloud Security Posture Management (CSPM), el administrador delegado pierde la capacidad de configurar el Security Hub CSPM, los estándares de seguridad y los controles de seguridad en varias Cuentas de AWS unidades organizativas () y. OUs Regiones de AWS En su lugar, debe configurar la mayoría de los ajustes por separado para cada cuenta en cada región.

Important

Antes de poder deshabilitar la configuración central, primero debe [desasociar sus cuentas y su](#) configuración actual, ya sea que se trate OUs de una política de configuración o de un comportamiento autogestionado.

Antes de poder deshabilitar la configuración centralizada, también debe [eliminar las políticas de configuración existentes](#).

Al deshabilitar la configuración centralizada, se producen los siguientes cambios:

- El administrador delegado ya no puede crear políticas de configuración para la organización.
- Las cuentas que tenían una política de configuración aplicada o heredada retienen su configuración actual, pero se vuelven autoadministradas.
- Su organización cambia a la configuración local. En la configuración local, la mayoría de los ajustes de CSPM de Security Hub deben configurarse por separado en cada cuenta y región de la organización. El administrador delegado puede optar por habilitar automáticamente el Security Hub CSPM, los [estándares de seguridad predeterminados](#) y todos los controles que forman parte de los estándares predeterminados en las nuevas cuentas de la organización. Los estándares predeterminados son AWS Foundational Security Best Practices (FSBP) y Center for Internet Security (CIS) Foundations Benchmark v1.2.0. AWS Esta configuración entra en vigor en la región actual y afecta únicamente a las cuentas nuevas de la organización. El administrador delegado no puede cambiar los estándares predeterminados. La configuración local no admite el uso de políticas de configuración ni la configuración a nivel de la unidad organizativa.

La identidad de la cuenta de administrador delegado sigue siendo la misma cuando se deja de utilizar la configuración centralizada. Su región de origen y las regiones vinculadas también siguen siendo las mismas (su región de origen ahora se denomina región de agregación y se puede utilizar para la agregación de resultados).

Elija el método que prefiera y siga los pasos para dejar de utilizar la configuración centralizada y cambiar a la configuración local.

Security Hub CSPM console

Para deshabilitar la configuración centralizada (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>.

Inicie sesión con las credenciales de la cuenta de administrador CSPM de Security Hub delegada en la región de origen.
2. En el panel de navegación, seleccione Configuración y Configuración.
3. En la sección Información general, seleccione Editar.
4. En el cuadro Editar configuración de la organización, seleccione Configuración local. Si aún no lo ha hecho, se le solicitará que desasocie y elimine las políticas de configuración actuales antes de poder dejar de utilizar la configuración centralizada. Las cuentas o OUs que estén designadas como autogestionadas deben disociarse de su configuración autogestionada. Para ello, en la consola puede [cambiar el tipo de administración](#) de cada cuenta u unidad organizativa autoadministrada a Administrada de forma centralizada y Heredar de mi organización.
5. Si lo desea, seleccione los ajustes predeterminados de la configuración local para las nuevas cuentas de la organización.
6. Elija Confirmar.

Security Hub CSPM API

Para deshabilitar la configuración centralizada (API)

1. Invoque la API [UpdateOrganizationConfiguration](#).
2. Establezca el campo `ConfigurationType` del objeto `OrganizationConfiguration` en `LOCAL`. La API devuelve un error si tiene políticas de configuración o asociaciones

de políticas existentes. Para desasociar una política de configuración, invoque la API `StartConfigurationPolicyDisassociation`. Para eliminar una política de configuración, invoque la API `DeleteConfigurationPolicy`.

3. Si quieres activar automáticamente el CSPM de Security Hub en las nuevas cuentas de la organización, establece el `AutoEnable` campo en `true`. De forma predeterminada, el valor de este campo es `false` y Security Hub CSPM no se habilita automáticamente en las nuevas cuentas de la organización. De forma opcional, si quiere habilitar automáticamente Security Hub en las nuevas cuentas de la organización, establezca el campo `AutoEnableStandards` en `DEFAULT`. Este es el valor predeterminado. Si no quiere habilitar automáticamente los estándares de seguridad predeterminados en las nuevas cuentas de la organización, establezca el campo `AutoEnableStandards` en `NONE`.

Ejemplo de solicitud de API:

```
{
  "AutoEnable": true,
  "OrganizationConfiguration": {
    "ConfigurationType" : "LOCAL"
  }
}
```

AWS CLI

Para deshabilitar la configuración centralizada (AWS CLI)

1. Ejecute el comando [update-organization-configuration](#).
2. Establezca el campo `ConfigurationType` del objeto `organization-configuration` en `LOCAL`. El comando devuelve un error si tiene políticas de configuración o asociaciones de políticas existentes. Para desasociar una política de configuración, ejecute el comando `start-configuration-policy-disassociation`. Para eliminar una política de configuración, ejecute el comando `delete-configuration-policy`.
3. Si desea habilitar automáticamente el CSPM de Security Hub en las nuevas cuentas de la organización, incluya el `auto-enable` parámetro. De forma predeterminada, el valor de este parámetro es `no-auto-enable` y el CSPM de Security Hub no se habilita automáticamente en las nuevas cuentas de la organización. De forma opcional, si quiere habilitar automáticamente Security Hub en las nuevas cuentas de la organización, establezca

el campo `auto-enable-standards` en `DEFAULT`. Este es el valor predeterminado. Si no quiere habilitar automáticamente los estándares de seguridad predeterminados en las nuevas cuentas de la organización, establezca el campo `auto-enable-standards` en `NONE`.

```
aws securityhub --region us-east-1 update-organization-configuration \  
--auto-enable \  
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

Administrar las cuentas de administrador y miembro en Security Hub (CSPM)

Si su AWS entorno tiene varias cuentas, puede tratar las cuentas que utilizan AWS Security Hub Cloud Security Posture Management (CSPM) como cuentas de miembros y asociarlas a una sola cuenta de administrador. El administrador puede supervisar el estado general de seguridad y tomar [medidas permitidas](#) en las cuentas de miembro. El administrador también puede realizar diversas tareas de gestión y administración de cuentas a gran escala, como supervisar los costos de uso estimados y evaluar las cuotas de las cuentas.

Puede asociar las cuentas de los miembros a un administrador de dos maneras: integrando Security Hub CSPM AWS Organizations o enviando y aceptando manualmente las invitaciones de membresía en Security Hub CSPM.

Administrar cuentas con AWS Organizations

AWS Organizations es un servicio de administración de cuentas global que permite a AWS los administradores consolidar y administrar múltiples cuentas. Cuentas de AWS 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 AWS Security Hub Cloud Security Posture Management (CSPM), Amazon Macie y Amazon GuardDuty. Para obtener más información, consulte la [Guía del usuario de AWS Organizations](#).

Al integrar Security Hub CSPM y AWS Organizations, la cuenta de administración de Organizations designa a un administrador delegado de Security Hub CSPM. El CSPM de Security Hub se habilita automáticamente en la cuenta de administrador delegado Región de AWS en la que se designó.

[Tras designar un administrador delegado, se recomienda administrar las cuentas en Security Hub CSPM con una configuración central.](#) Esta es la forma más eficaz de personalizar Security Hub CSPM y garantizar una cobertura de seguridad adecuada para su organización.

La configuración central permite al administrador delegado personalizar el CSPM de Security Hub en varias cuentas y regiones de la organización en lugar de configurarlo. Region-by-Region Puede crear una política de configuración para toda la organización o crear políticas de configuración diferentes para diferentes cuentas y. OUs Las políticas especifican si Security Hub CSPM está habilitado o deshabilitado en las cuentas asociadas y qué estándares y controles de seguridad están habilitados.

El administrador delegado puede designar las cuentas como administradas de manera centralizada o autoadministradas. Las cuentas administradas de manera centralizada solo las puede configurar el administrador delegado. Las cuentas autoadministradas pueden especificar su propia configuración.

Si no opta por la configuración central, el administrador delegado tiene una capacidad más limitada para configurar el Security Hub CSPM, lo que se denomina configuración local. En la configuración local, el administrador delegado puede habilitar automáticamente el Security Hub CSPM y los [estándares de seguridad predeterminados](#) en las nuevas cuentas de la organización en la región actual. Sin embargo, las cuentas existentes no utilizan esta configuración, por lo que se pueden producir cambios en la configuración después de que una cuenta se una a la organización.

Además de esta nueva configuración de la cuenta, la configuración local es específica de la cuenta y de la región. Cada cuenta de la organización debe configurar el servicio CSPM, los estándares y los controles de Security Hub por separado en cada región. La configuración local tampoco admite el uso de políticas de configuración.

Administración manual de cuentas mediante invitación

Debe administrar manualmente las cuentas de los miembros mediante invitación en Security Hub CSPM si tiene una cuenta independiente o si no se integra con Organizations. Una cuenta independiente no se puede integrar con Organizations, por lo que es necesario administrarla manualmente. Recomendamos la integración AWS Organizations y el uso de la configuración central si agrega cuentas adicionales en el futuro.

Cuando utiliza la administración manual de cuentas, designa una cuenta como administradora de CSPM de Security Hub. La cuenta de administrador puede ver los datos de las cuentas de miembro y tomar determinadas medidas en función de los resultados de las cuentas de miembro. El administrador de Security Hub CSPM invita a otras cuentas a ser cuentas de miembros, y la relación administrador-miembro se establece cuando una cuenta de miembro potencial acepta la invitación.

La administración manual de cuentas no admite el uso de políticas de configuración. Sin políticas de configuración, el administrador no puede personalizar de forma centralizada el CSPM de Security Hub configurando parámetros variables para diferentes cuentas. En su lugar, cada cuenta de la organización debe habilitar y configurar el Security Hub CSPM por sí misma por separado en cada región. Esto puede hacer que sea más difícil y lento garantizar una cobertura de seguridad adecuada en todas las cuentas y regiones en las que utilice Security Hub CSPM. También puede provocar cambios en la configuración, ya que las cuentas de miembro pueden especificar su propia configuración sin la intervención del administrador.

Para administrar las cuentas mediante invitación, consulte [Administrar cuentas por invitación en Security Hub \(CSPM\)](#).

Recomendaciones para administrar varias cuentas en Security Hub (CSPM)

En la siguiente sección se resumen algunas restricciones y recomendaciones que se deben tener en cuenta al gestionar las cuentas de los miembros en AWS Security Hub Cloud Security Posture Management (CSPM).

Número máximo de cuentas miembro

Si utilizas la integración con AWS Organizations, Security Hub CSPM admite hasta 10 000 cuentas de miembros por cuenta de administrador delegado en cada una de ellas. Región de AWS Si habilita y administra Security Hub CSPM manualmente, Security Hub CSPM admite hasta 1000 invitaciones de cuentas de miembros por cuenta de administrador en cada región.

Creación de relaciones administrador-miembro

Note

Si utilizas la integración CSPM de Security Hub con AWS Organizations una cuenta de miembro y no has invitado manualmente a ninguna cuenta de miembro, esta sección no se aplica a ti.

Una cuenta no puede ser cuenta de administrador y cuenta de miembro al mismo tiempo.

Una cuenta miembro solo se puede asociar con una cuenta de administrador. Si la cuenta de administrador CSPM de Security Hub habilita una cuenta de organización, la cuenta no podrá aceptar una invitación de otra cuenta. Si una cuenta ya ha aceptado una invitación, la cuenta de administrador de CSPM de Security Hub de la organización no podrá habilitarla. Tampoco puede recibir invitaciones de otras cuentas.

En el caso del proceso de invitación manual, aceptar una invitación para convertirse en miembro es opcional.

Membresía mediante AWS Organizations

Si integra Security Hub CSPM con AWS Organizations, la cuenta de administración de la organización puede designar una cuenta de administrador delegado (DA) para Security Hub CSPM. En Organizations, la cuenta de administración de la organización no se puede configurar como el administrador delegado. Si bien esto está permitido en Security Hub CSPM, recomendamos que la cuenta de administración de Organizations no sea la DA.

Le recomendamos que seleccione la misma cuenta de administrador delegado en todas las regiones. Si usa la [configuración central](#), Security Hub CSPM establece la misma cuenta DA en todas las regiones en las que configura Security Hub CSPM para su organización.

También le recomendamos que elija la misma cuenta DA en todos los servicios de AWS seguridad y cumplimiento para ayudarlo a gestionar los problemas relacionados con la seguridad desde un único panel de control.

Membresía por invitación

En el caso de las cuentas miembro creadas mediante invitación, la asociación de cuentas administrador-miembro se crea únicamente en la región desde la que se envía la invitación. La cuenta de administrador debe habilitar el CSPM de Security Hub en cada región en la que desee usarla. A continuación, la cuenta de administrador invita a cada cuenta a convertirse en cuenta de miembro en esa región.

Note

Recomendamos utilizar, AWS Organizations en lugar de Security Hub, invitaciones CSPM para gestionar las cuentas de los miembros.

Coordinar cuentas de administrador en todos los servicios

Security Hub CSPM agrega los hallazgos de varios AWS servicios, como Amazon, Amazon GuardDuty Inspector y Amazon Macie. Security Hub CSPM también permite a los usuarios pasar de un GuardDuty hallazgo a iniciar una investigación en Amazon Detective.

Sin embargo, las relaciones administrador-miembro que se configuran en estos otros servicios no se aplican automáticamente a Security Hub CSPM. Security Hub CSPM recomienda utilizar la misma cuenta que la cuenta de administrador para todos estos servicios. Esta cuenta de administrador debe

ser una cuenta responsable de las herramientas de seguridad. La misma cuenta también debe ser la cuenta de agregador de AWS Config.

Por ejemplo, un usuario de la cuenta de GuardDuty administrador A puede ver los resultados de las cuentas de GuardDuty los miembros B y C en la GuardDuty consola. Si la cuenta A activa el CSPM de Security Hub, los usuarios de la cuenta A no ven automáticamente los GuardDuty resultados de las cuentas B y C en Security Hub CSPM. También se requiere una relación administrador-miembro de Security Hub CSPM para estas cuentas.

Para ello, convierta la cuenta A en la cuenta de administrador de CSPM de Security Hub y habilite las cuentas B y C para que se conviertan en cuentas miembros de Security Hub CSPM.

Administrar Security Hub CSPM para varias cuentas con AWS Organizations

Puede integrar AWS Security Hub Cloud Security Posture Management (CSPM) con Security Hub CSPM y AWS Organizations, a continuación, administrar el Security Hub CSPM para las cuentas de su organización.

Para integrar Security Hub CSPM con AWS Organizations, debe crear una organización en. AWS Organizations La cuenta de administración de Organizations designa una cuenta como administrador delegado de CSPM de Security Hub para la organización. A continuación, el administrador delegado puede habilitar Security Hub CSPM para otras cuentas de la organización, añadir esas cuentas como cuentas de miembros de Security Hub CSPM y realizar las acciones permitidas en las cuentas de los miembros. El administrador delegado de Security Hub CSPM puede habilitar y administrar Security Hub CSPM para hasta 10 000 cuentas de miembros.

El alcance de las capacidades de configuración del administrador delegado depende de si utiliza la [configuración centralizada](#). Con la configuración central habilitada, no necesita configurar Security Hub CSPM por separado en cada cuenta de miembro y. Región de AWS El administrador delegado puede aplicar ajustes específicos de CSPM de Security Hub en determinadas cuentas de miembros y unidades organizativas (OUs) de todas las regiones.

La cuenta de administrador delegado CSPM de Security Hub puede realizar las siguientes acciones en las cuentas de los miembros:

- Si utiliza una configuración central, configure el Security Hub CSPM de forma centralizada para las cuentas de los miembros y cree políticas OUs de configuración del Security Hub CSPM. Las

políticas de configuración se pueden usar para habilitar y deshabilitar Security Hub CSPM, habilitar y deshabilitar los estándares y habilitar y deshabilitar los controles.

- Trate automáticamente las cuentas nuevas como cuentas de miembros de Security Hub CSPM cuando se unan a la organización. Si utiliza la configuración centralizada, una política de configuración asociada a una unidad organizativa incluye las cuentas nuevas y existentes que forman parte de la unidad organizativa.
- Trate las cuentas de la organización existentes como cuentas de miembros de Security Hub CSPM. Esto ocurre automáticamente si utiliza una configuración centralizada.
- Desasociar las cuentas miembro que pertenecen a la organización. Si utiliza la configuración centralizada, solo podrá desasociar una cuenta de miembro después de designarla como autoadministrada. Como alternativa, puede asociar una política de configuración que deshabilite el CSPM de Security Hub con cuentas de miembro específicas administradas centralmente.

Si no opta por la configuración centralizada, su organización utilizará el tipo de configuración predeterminada denominada configuración local. En la configuración local, el administrador delegado tiene una capacidad más limitada para aplicar la configuración en las cuentas de miembro. Para obtener más información, consulte [Descripción de la configuración local en Security Hub \(CSPM\)](#).

Para obtener una lista completa de las acciones que el administrador delegado puede llevar a cabo en las cuentas de los miembros, consulte [Acciones permitidas por parte del administrador y las cuentas de los miembros en Security Hub \(CSPM\)](#).

En los temas de esta sección se explica cómo integrar el Security Hub CSPM AWS Organizations y cómo administrar el Security Hub CSPM para las cuentas de una organización. Cuando proceda, en cada sección, se identifican las ventajas y diferencias de administración para los usuarios de la configuración centralizada.

Temas

- [Integración de Security Hub CSPM con AWS Organizations](#)
- [Activación automática de Security Hub CSPM en las nuevas cuentas de la organización](#)
- [Activación manual de Security Hub CSPM en las nuevas cuentas de la organización](#)
- [Desasociar las cuentas de los miembros de Security Hub CSPM de su organización](#)

Integración de Security Hub CSPM con AWS Organizations

Para integrar AWS Security Hub Cloud Security Posture Management (CSPM) y AWS Organizations, debe crear una organización en Organizations y utilizar la cuenta de administración de la organización para designar una cuenta de administrador delegada de Security Hub CSPM. Esto hace que Security Hub CSPM sea un servicio de confianza en Organizations. [También habilita el CSPM de Security Hub en la cuenta actual Región de AWS de administrador delegado y permite al administrador delegado habilitar el CSPM de Security Hub para las cuentas de los miembros, ver los datos de las cuentas de los miembros y realizar otras acciones permitidas en las cuentas de los miembros.](#)

Si utiliza la [configuración central](#), el administrador delegado también puede crear políticas de configuración de CSPM del Security Hub que especifiquen cómo se deben configurar el servicio, los estándares y los controles de CSPM del Security Hub en las cuentas de la organización.

Creación de una organización

Una organización es una entidad que se crea para consolidarla y Cuentas de AWS poder administrarla como una sola unidad.

Puede crear una organización mediante la AWS Organizations consola o mediante un comando del SDK AWS CLI o de uno de ellos APIs. Para obtener instrucciones detalladas sobre cómo hacerlo, consulte [Creación de una organización](#) en la Guía del usuario de AWS Organizations .

Puede utilizarla AWS Organizations para ver y gestionar de forma centralizada todas las cuentas de su organización. Una organización tiene una cuenta de administración junto con cero o más cuentas miembro. Puedes organizar las cuentas en una estructura jerárquica similar a un árbol con una raíz en la parte superior y unidades organizativas (OUs) anidadas debajo de la raíz. Cada cuenta puede estar directamente debajo de la raíz o colocarse en una de las siguientes jerarquías. OUs Una unidad organizativa es un contenedor para cuentas específicas. Por ejemplo, puede crear una unidad organizativa de finanzas que incluya todas las cuentas relacionadas con las operaciones financieras.

Recomendaciones para elegir al administrador delegado de Security Hub (CSPM)

Si dispone de una cuenta de administrador gracias al proceso de invitación manual y está realizando la transición a la administración de cuentas con ella AWS Organizations, le recomendamos que designe esa cuenta como administrador delegado de CSPM de Security Hub.

Aunque el CSPM APIs y la consola del Security Hub permiten que la cuenta de administración de la organización sea el administrador delegado del CSPM del Security Hub, se recomienda elegir dos cuentas diferentes. Esto se debe a que es probable que los usuarios que tienen acceso a la cuenta de administración de la organización para administrar la facturación sean diferentes de los usuarios que necesitan acceso a Security Hub CSPM para la administración de la seguridad.

Le recomendamos que utilice el mismo administrador delegado en todas las regiones. Si opta por la configuración central, Security Hub CSPM designa automáticamente al mismo administrador delegado en su región de origen y en cualquier región vinculada.

Verificación de permisos para configurar al administrador delegado

Para designar y eliminar una cuenta de administrador de CSPM de Security Hub delegada, la cuenta de administración de la organización debe tener permisos `EnableOrganizationAdminAccount` y `DisableOrganizationAdminAccount` acciones en Security Hub CSPM. La cuenta de administración de Organizations también debe contar con permisos administrativos para Organizations.

Para conceder todos los permisos necesarios, adjunte las siguientes políticas gestionadas por CSPM de Security Hub al principal de IAM de la cuenta de administración de la organización:

- [AWSSecurityHubFullAccess](#)
- [AWSSecurityHubOrganizationsAccess](#)

Designación del administrador delegado

Para designar la cuenta de administrador CSPM de Security Hub delegada, puede utilizar la consola CSPM de Security Hub, la API CSPM de Security Hub o. AWS CLI Security Hub CSPM establece el administrador delegado Región de AWS solo en la actual, y debe repetir la acción en otras regiones. Si comienza a utilizar la configuración central, Security Hub CSPM establece automáticamente el mismo administrador delegado en la región de origen y en las regiones vinculadas.

La cuenta de administración de la organización no tiene que habilitar el CSPM de Security Hub para designar la cuenta de administrador del CSPM de Security Hub delegada.

Recomendamos que la cuenta de administración de la organización no sea la cuenta de administrador de CSPM de Security Hub delegada. Sin embargo, si elige la cuenta de administración de la organización como administrador delegado de CSPM de Security Hub, la cuenta de administración debe tener activado Security Hub CSPM. Si la cuenta de administración no tiene

el Security Hub CSPM activado, debe habilitar el Security Hub CSPM para ella manualmente. El CSPM de Security Hub no se puede habilitar automáticamente para la cuenta de administración de la organización.

Debe designar al administrador CSPM de Security Hub delegado mediante uno de los siguientes métodos. La designación del administrador de CSPM de Security Hub delegado con Organizations APIs no se refleja en Security Hub CSPM.

Elija el método que prefiera y siga los pasos para designar la cuenta de administrador de CSPM de Security Hub delegada.

Security Hub CSPM console

Para designar al administrador delegado durante el proceso de incorporación

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. Selecciona Ir a Security Hub CSPM. Se le solicitará que inicie sesión en la cuenta de administración de la organización.
3. En la página Designar administrador delegado, en la sección Cuenta de administrador delegado, especifique la cuenta de administrador delegado. Se recomienda que elija el mismo administrador delegado que haya configurado para otros servicios de seguridad y conformidad de AWS .
4. Elija Establecer administrador delegado. Se le solicitará que inicie sesión en la cuenta de administrador delegado (si aún no lo ha hecho) para continuar con la integración con la configuración centralizada. Si no desea iniciar la configuración centralizada, seleccione Cancelar. Su administrador delegado está configurado, pero usted todavía no utiliza la configuración centralizada.

Para designar al administrador delegado desde la página Configuración

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación CSPM de Security Hub, elija Configuración. A continuación, elija General.
3. Si actualmente hay asignada una cuenta de administrador CSPM de Security Hub, antes de poder designar una nueva cuenta, debe eliminar la cuenta actual.

En Administrador delegado, para eliminar la cuenta actual, seleccione Eliminar.

4. Introduzca el ID de cuenta de la cuenta que desee designar como cuenta de administrador de CSPM de Security Hub.

Debe designar la misma cuenta de administrador CSPM de Security Hub en todas las regiones. Si designa una cuenta diferente de la que ha designado en otras regiones, la consola le mostrará un error.

5. Elija Delegar.

Security Hub CSPM API, AWS CLI

Desde la cuenta de administración de la organización, utilice la [EnableOrganizationAdminAccount](#) operación de la API CSPM de Security Hub. Si utiliza la AWS CLI, ejecute el comando [enable-organization-admin-account](#). Proporcione el Cuenta de AWS ID del administrador de CSPM de Security Hub delegado.

El siguiente ejemplo designa al administrador CSPM de Security Hub delegado. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub enable-organization-admin-account --admin-account-id 123456789012
```

Eliminación o cambio del administrador delegado

Solo la cuenta de administración de la organización puede eliminar la cuenta de administrador de CSPM de Security Hub delegada.

Para cambiar el administrador CSPM de Security Hub delegado, primero debe eliminar la cuenta de administrador delegado actual y, a continuación, designar una nueva.

Warning

Cuando usa la [configuración central](#), no puede usar la consola CSPM de Security Hub ni la CSPM de Security Hub APIs para cambiar o eliminar la cuenta de administrador delegado. Si la cuenta de administración de la organización usa la AWS Organizations consola o AWS Organizations APIs para cambiar o eliminar el administrador de CSPM de Security Hub delegado, Security Hub CSPM detiene automáticamente la configuración central y elimina

las políticas de configuración y las asociaciones de políticas. Las cuentas de los miembros retienen la configuración que tenían antes de que se cambiara o eliminara el administrador delegado.

Si utiliza la consola CSPM de Security Hub para eliminar al administrador delegado en una región, se eliminará automáticamente en todas las regiones.

La API CSPM de Security Hub solo elimina la cuenta de administrador de CSPM de Security Hub delegada de la región en la que se emite la llamada o el comando a la API. Debe repetir la acción en las demás regiones.

Si utiliza la API de Organizations para eliminar la cuenta de administrador de CSPM de Security Hub delegada, se eliminará automáticamente en todas las regiones.

Eliminar el administrador delegado (Organizations API, AWS CLI)

Puede usar Organizations para eliminar al administrador delegado de CSPM de Security Hub en todas las regiones.

Si utiliza la configuración centralizada para administrar las cuentas, al eliminar la cuenta de administrador delegado, se eliminarán las políticas de configuración y las asociaciones de políticas. Las cuentas de miembro retienen las configuraciones que tenían antes de que se cambiara o eliminara el administrador delegado. Sin embargo, la cuenta de administrador delegado eliminada ya no puede administrar estas cuentas. Se convierten en cuentas autoadministradas que deben configurarse por separado en cada región.

Elija el método que prefiera y siga las instrucciones para eliminar la cuenta de administrador de CSPM de Security Hub delegada con ella. AWS Organizations

Organizations API, AWS CLI

Para eliminar el administrador delegado de Security Hub (CSPM)

Desde la cuenta de administración de la organización, use la operación [DeregisterDelegatedAdministrator](#) de la API de Organizations. Si utiliza la AWS CLI, ejecute el comando [deregister-delegated-administrator](#). Proporcione el ID de cuenta del administrador delegado y el principal de servicio de Security Hub CSPM, que es. `securityhub.amazonaws.com`

En el siguiente ejemplo, se elimina el administrador CSPM de Security Hub delegado. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws organizations deregister-delegated-administrator --account-id 123456789012 --service-principal securityhub.amazonaws.com
```

Eliminar el administrador delegado (consola CSPM de Security Hub)

Puede usar la consola CSPM de Security Hub para eliminar al administrador de CSPM de Security Hub delegado en todas las regiones.

Cuando se elimina la cuenta de administrador de CSPM de Security Hub delegada, las cuentas de los miembros se disocian de la cuenta de administrador de CSPM de Security Hub delegada eliminada.

El CSPM de Security Hub sigue activado en las cuentas de los miembros. Se convierten en cuentas independientes hasta que un nuevo administrador de Security Hub CSPM las habilite como cuentas de miembros.

Si la cuenta de administración de la organización no es una cuenta habilitada en Security Hub CSPM, utilice la opción de la página Bienvenido a Security Hub CSPM.

Para eliminar la cuenta de administrador de Security Hub (CSPM) delegada de la página de bienvenida a Security Hub (CSPM)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. Seleccione Ir a Security Hub.
3. En Administrador delegado, seleccione Eliminar.

Si la cuenta de administración de la organización es una cuenta habilitada en Security Hub, utilice la opción de la pestaña General de la página Configuración.

Para eliminar la cuenta de administrador CSPM de Security Hub delegada de la página de configuración

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>

2. En el panel de navegación CSPM de Security Hub, elija Configuración. A continuación, elija General.
3. En Administrador delegado, seleccione Eliminar.

Eliminar el administrador delegado (API CSPM de Security Hub,) AWS CLI

Puede utilizar la API CSPM de Security Hub o las operaciones CSPM de Security Hub para eliminar AWS CLI al administrador de CSPM de Security Hub delegado. Al eliminar al administrador delegado con uno de estos métodos, este solo se elimina en la región en la que se emitió el comando o la llamada a la API. Security Hub CSPM no actualiza otras regiones ni elimina la cuenta de administrador delegado en ellas. AWS Organizations

Elija el método que prefiera y siga estos pasos para eliminar la cuenta de administrador de CSPM de Security Hub delegada con Security Hub CSPM.

Security Hub CSPM API, AWS CLI

Para eliminar el administrador delegado de Security Hub (CSPM)

Desde la cuenta de administración de la organización, utilice la [DisableOrganizationAdminAccount](#) operación de la API CSPM de Security Hub. Si está utilizando el AWS CLI, ejecute el [disable-organization-admin-account](#) comando. Proporcione el ID de cuenta del administrador de CSPM de Security Hub delegado.

En el siguiente ejemplo, se elimina el administrador CSPM de Security Hub delegado. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

Desactivar la integración de Security Hub CSPM con AWS Organizations

Una vez que una AWS Organizations organización se ha integrado con AWS Security Hub Cloud Security Posture Management (CSPM), la cuenta de administración de Organizations puede deshabilitar posteriormente la integración. Como usuario de la cuenta de administración de Organizations, puede hacerlo deshabilitando el acceso de confianza para el CSPM de Security Hub en. AWS Organizations

Al deshabilitar el acceso de confianza para Security Hub CSPM, ocurre lo siguiente:

- Security Hub CSPM pierde su condición de servicio de confianza en. AWS Organizations
- La cuenta de administrador delegado de CSPM de Security Hub pierde el acceso a la configuración, los datos y los recursos de todas las cuentas de los miembros de Security Hub CSPM. Regiones de AWS
- Si utilizaba una [configuración central](#), Security Hub CSPM deja de usarla automáticamente en su organización. Se eliminan las políticas de configuración y las asociaciones de políticas. Las cuentas retienen las configuraciones que tenían antes de deshabilitar el acceso de confianza.
- Todas las cuentas de los miembros de Security Hub CSPM se convierten en cuentas independientes y conservan su configuración actual. Si el CSPM de Security Hub estaba habilitado para una cuenta de miembro en una o más regiones, el CSPM de Security Hub seguirá estando habilitado para la cuenta en esas regiones. Los estándares y controles habilitados tampoco se modifican. Puede modificar esta configuración por separado en cada cuenta y región. Sin embargo, la cuenta ya no está asociada a un administrador delegado en ninguna región.

Para obtener información adicional sobre los resultados de la desactivación del acceso a un servicio de confianza, consulte [Uso AWS Organizations con otros Servicios de AWS](#) en la Guía del usuario.AWS Organizations

Para deshabilitar el acceso de confianza, puede usar la AWS Organizations consola, la API de Organizations o la AWS CLI. Solo un usuario de la cuenta de administración de Organizations puede deshabilitar el acceso a servicios de confianza para Security Hub CSPM. Para obtener más información sobre los permisos que necesita, consulte [Permisos necesarios para deshabilitar el acceso de confianza](#) en la Guía del usuario de AWS Organizations .

Antes de deshabilitar el acceso de confianza, le recomendamos que trabaje con el administrador delegado de su organización para deshabilitar el Security Hub CSPM en las cuentas de los miembros y limpiar los recursos del Security Hub CSPM en esas cuentas.

Elige el método que prefieras y sigue los pasos para deshabilitar el acceso de confianza para Security Hub CSPM.

Organizations console

Para deshabilitar el acceso de confianza para Security Hub (CSPM)

1. Inicie sesión con las AWS Management Console credenciales de la cuenta de AWS Organizations administración.
2. Abra la consola de Organizations en <https://console.aws.amazon.com/organizations/>.

3. En el panel de navegación, elija Servicios.
4. En Servicios integrados, elija AWS Security Hub Cloud Security Posture Management (CSPM).
5. Seleccione Deshabilitar el acceso de confianza.
6. Confirme que desea deshabilitar el acceso de confianza.

Organizations API

Para deshabilitar el acceso de confianza para Security Hub (CSPM)

Invoque la operación de [inhabilitación del AWSService acceso](#) de la API. AWS Organizations Para el `ServicePrincipal` parámetro, especifique el principal de servicio CSPM de Security Hub (`()securityhub.amazonaws.com`).

AWS CLI

Para deshabilitar el acceso de confianza para Security Hub (CSPM)

Ejecute el [disable-aws-service-access](#) comando de la AWS Organizations API. Para el `service-principal` parámetro, especifique el principal de servicio CSPM de Security Hub (`()securityhub.amazonaws.com`).

Ejemplo:

```
aws organizations disable-aws-service-access --service-principal
securityhub.amazonaws.com
```

Activación automática de Security Hub CSPM en las nuevas cuentas de la organización

Cuando se incorporan nuevas cuentas a su organización, se añaden a la lista de la página Cuentas de la consola AWS Security Hub Cloud Security Posture Management (CSPM). En el caso de las cuentas de la organización, el Tipo es Por organización. De forma predeterminada, las cuentas nuevas no se convierten en miembros de Security Hub CSPM cuando se unen a la organización. Su estado es No es miembro. La cuenta de administrador delegado puede añadir automáticamente nuevas cuentas como miembros y habilitar Security Hub CSPM en estas cuentas cuando se unan a la organización.

 Note

Aunque muchas de Regiones de AWS ellas están activas de forma predeterminada Cuenta de AWS, debe activar algunas regiones de forma manual. En el presente documento estas regiones se denominan regiones de suscripción voluntaria. Para habilitar automáticamente el CSPM de Security Hub en una cuenta nueva de una región que haya optado por participar, la cuenta debe tener esa región activada primero. Solo el propietario de la cuenta puede activar la región de suscripción voluntaria. Para obtener más información sobre las regiones de suscripción voluntaria, consulte [Especificar qué puede usar Regiones de AWS su cuenta](#).

Este proceso es diferente en función de si se utiliza la configuración centralizada (recomendada) o la configuración local.

Habilitación automática de nuevas cuentas de la organización (configuración centralizada)

Si usa la [configuración central](#), puede habilitar automáticamente el CSPM de Security Hub en las cuentas nuevas y existentes de la organización mediante la creación de una política de configuración en la que esté habilitado el CSPM de Security Hub. A continuación, puede asociar la política a la raíz de la organización o a unidades organizativas específicas (). OUs

Si asocia una política de configuración en la que el CSPM de Security Hub esté habilitado a una OU específica, el CSPM de Security Hub se habilita automáticamente en todas las cuentas (existentes y nuevas) que pertenecen a esa OU. Las cuentas nuevas que no pertenecen a la OU se autoadministran y no tienen activado automáticamente el CSPM de Security Hub. Si asocia una política de configuración en la que el CSPM de Security Hub esté habilitado con la raíz, el CSPM de Security Hub se habilita automáticamente en todas las cuentas (existentes y nuevas) que se unan a la organización. Las excepciones son si una cuenta usa una política diferente por aplicación o herencia, o si es autoadministrada.

En su política de configuración, también puede definir qué estándares y controles de seguridad deben habilitarse en la unidad organizativa. Para generar resultados de control para los estándares habilitados, las cuentas de la OU deben estar AWS Config habilitadas y configuradas para registrar los recursos necesarios. Para obtener más información sobre el AWS Config registro, consulte [Habilitación y configuración AWS Config](#).

Para obtener instrucciones sobre cómo crear una política de configuración, consulte [Creación y asociación de políticas de configuración](#).

Habilitación automática de nuevas cuentas de la organización (configuración local)

Al utilizar la configuración local y activar la activación automática de los estándares predeterminados, Security Hub CSPM agrega nuevas cuentas de la organización como miembros y habilita el Security Hub CSPM en ellas en la región actual. Otras regiones no se ven afectadas. Además, activar la activación automática no habilita el CSPM de Security Hub en las cuentas de la organización existentes, a menos que ya se hayan agregado como cuentas de miembros.

Después de activar la habilitación automática, los estándares de seguridad predeterminados se habilitan para las cuentas de miembro nuevas en la región actual cuando se unen a la organización. Los estándares predeterminados son AWS Foundational Security Best Practices (FSBP) y Center for Internet Security (CIS) Foundations Benchmark v1.2.0. AWS No puede cambiar los estándares predeterminados. Si desea habilitar otros estándares en toda su organización o habilitar los estándares para determinadas cuentas, le recomendamos que utilice la configuración OUs central.

Para generar resultados de control para los estándares predeterminados (y otros estándares habilitados), las cuentas de su organización deben estar AWS Config habilitadas y configuradas para registrar los recursos necesarios. Para obtener más información sobre el AWS Config registro, consulte [Habilitar y configurar AWS Config](#).

Elige el método que prefieras y sigue los pasos para habilitar automáticamente el CSPM de Security Hub en las nuevas cuentas de la organización. Estas instrucciones solo se aplican si utiliza la configuración local.

Security Hub CSPM console

Para habilitar automáticamente las nuevas cuentas de la organización como miembros de Security Hub (CSPM)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>

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

2. En el panel de navegación CSPM de Security Hub, en Configuración, elija Configuración.
3. En la sección Cuentas, active Habilitación automática de cuentas.

Security Hub CSPM API

Para habilitar automáticamente las nuevas cuentas de la organización como miembros de Security Hub (CSPM)

invoque la API [UpdateOrganizationConfiguration](#) desde la cuenta de administrador delegado. Defina el `AutoEnable` campo en `true` para habilitar automáticamente el CSPM de Security Hub en las nuevas cuentas de la organización.

AWS CLI

Para habilitar automáticamente las nuevas cuentas de la organización como miembros de Security Hub (CSPM)

Ejecute el comando [update-organization-configuration](#) desde la cuenta de administrador delegado. Incluya el `auto-enable` parámetro para habilitar automáticamente el CSPM de Security Hub en las nuevas cuentas de la organización.

```
aws securityhub update-organization-configuration --auto-enable
```

Activación manual de Security Hub CSPM en las nuevas cuentas de la organización

Si no habilitas automáticamente el CSPM de Security Hub en las nuevas cuentas de la organización cuando se unen a la organización, puedes añadir esas cuentas como miembros y habilitar el CSPM de Security Hub en ellas manualmente después de que se unan a la organización. También debe habilitar manualmente el CSPM de Security Hub si anteriormente Cuentas de AWS se desasoció de una organización.

Note

Esta sección no se aplica a su caso si utiliza la [configuración centralizada](#). Si utilizas la configuración central, puedes crear políticas de configuración que habiliten el CSPM de Security Hub en determinadas cuentas de miembros y unidades organizativas (OU). También puedes habilitar estándares y controles específicos en esas cuentas y OUs

No puedes habilitar el CSPM de Security Hub en una cuenta si ya es una cuenta de miembro de otra organización.

Tampoco puedes habilitar el CSPM de Security Hub en una cuenta que esté suspendida actualmente. Si intenta habilitar el servicio en una cuenta suspendida, el estado de la cuenta cambia a Cuenta suspendida.

- Si la cuenta no tiene activado el CSPM de Security Hub, el CSPM de Security Hub está activado en esa cuenta. El estándar AWS Foundational Security Best Practices (FSBP) y CIS AWS Foundations Benchmark v1.2.0 también están habilitados en la cuenta, a menos que desactive los estándares de seguridad predeterminados.

La excepción a esto es la cuenta de administración de Organizations. El CSPM de Security Hub no se puede habilitar automáticamente en la cuenta de administración de Organizations. Debe habilitar manualmente el CSPM de Security Hub en la cuenta de administración de Organizations antes de poder añadirlo como cuenta de miembro.

- Si la cuenta ya tiene el Security Hub CSPM activado, Security Hub CSPM no realiza ningún otro cambio en la cuenta. Solo habilita la membresía.

Para que el CSPM de Security Hub genere resultados de control, las cuentas de los miembros deben estar AWS Config habilitadas y configuradas para registrar los recursos necesarios. Para obtener más información, consulte [Habilitación y configuración de AWS Config](#).

Elige el método que prefieras y sigue los pasos para habilitar una cuenta de organización como cuenta de miembro de Security Hub CSPM.

Security Hub CSPM console

Para habilitar manualmente las cuentas de la organización como miembros de Security Hub (CSPM)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>

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

2. En el panel de navegación CSPM de Security Hub, en Configuración, elija Configuración.
3. En la lista Cuentas, seleccione cada cuenta de la organización que desee habilitar.
4. Elija Acciones y Agregar miembro.

Security Hub CSPM API

Para habilitar manualmente las cuentas de la organización como miembros de Security Hub (CSPM)

Invoque la API [CreateMembers](#) desde la cuenta de administrador delegado. Debe indicar el ID de cada cuenta que desee habilitar.

A diferencia del proceso de invitación manual, al invocar `CreateMembers` para habilitar una cuenta de la organización, no es necesario enviar una invitación.

AWS CLI

Para habilitar manualmente las cuentas de la organización como miembros de Security Hub (CSPM)

Ejecute el comando [create-members](#) desde la cuenta de administrador delegado. Debe indicar el ID de cada cuenta que desee habilitar.

A diferencia del proceso de invitación manual, al ejecutar `create-members` para habilitar una cuenta de la organización, no es necesario enviar una invitación.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

Ejemplo

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"}, {"AccountId": "123456789222"}]'
```

Desasociar las cuentas de los miembros de Security Hub CSPM de su organización

Para dejar de recibir y ver los resultados de una cuenta de miembro de AWS Security Hub Cloud Security Posture Management (CSPM), puede desasociar la cuenta de miembro de su organización.

Note

Si utiliza la [configuración centralizada](#), la desasociación funciona de forma diferente. Puede crear una política de configuración que deshabilite el CSPM de Security Hub en una o más cuentas de miembro administradas centralmente. Después de eso, estas cuentas seguirán

formando parte de la organización, pero no generarán conclusiones sobre el CSPM de Security Hub. Si utiliza la configuración centralizada, pero también tiene cuentas de miembro invitadas manualmente, puede desasociar una o más cuentas invitadas manualmente.

Las cuentas de los miembros que se administran mediante no AWS Organizations pueden disociar sus cuentas de la cuenta de administrador. Solo la cuenta de administrador puede desasociar cuentas de miembro.

Al desasociar una cuenta de miembro, esta no se elimina. En su lugar, la cuenta de miembro se elimina de la organización. La cuenta de miembro disociada pasa a ser independiente y ya no Cuenta de AWS se administra mediante la integración de CSPM de Security Hub. AWS Organizations

Elija el método que prefiera y siga los pasos para desasociar una cuenta de miembro de la organización.

Security Hub CSPM console

Desasociación de una cuenta de miembro de la organización

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
Inicie sesión con las credenciales de la cuenta de administrador delegado.
2. En el panel de navegación, en Configuración, elija Configuración.
3. En la sección Cuentas, seleccione las cuentas que desee desasociar. Si utiliza la configuración centralizada, puede seleccionar una cuenta invitada manualmente para desvincularla desde la pestaña *Invitation accounts*. Esta pestaña solo es visible si utiliza la configuración centralizada.
4. Seleccione Acciones y, a continuación, Desasociar cuenta.

Security Hub CSPM API

Desasociación de una cuenta de miembro de la organización

Invoke la API [DisassociateMembers](#) desde la cuenta de administrador delegado. Debe proporcionar los datos Cuenta de AWS IDs para que las cuentas de los miembros se desasocien. Para ver una lista de las cuentas de miembro, invoque la API [ListMembers](#).

AWS CLI

Desasociación de una cuenta de miembro de la organización

Ejecute el comando [>disassociate-members](#) desde la cuenta de administrador delegado. Debe proporcionar la información necesaria Cuenta de AWS IDs para que las cuentas de los miembros se desasocien. Para ver una lista de las cuentas de miembro, ejecute el comando [>list-members](#).

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

Ejemplo

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

También puede usar la AWS Organizations consola o AWS SDKs desasociar una cuenta de miembro de su organización. AWS CLI Para obtener más información, consulte [Eliminación de una cuenta miembro de la organización](#) en la Guía del usuario de AWS Organizations .

Administrar cuentas por invitación en Security Hub (CSPM)

Puede gestionar de forma centralizada varias cuentas de AWS Security Hub Cloud Security Posture Management (CSPM) de dos maneras: integrando Security Hub CSPM AWS Organizations o enviando y aceptando manualmente las invitaciones de membresía. Debe utilizar el proceso manual si tiene una cuenta independiente o no la integra. AWS Organizations En la administración manual de cuentas, el administrador CSPM de Security Hub invita a las cuentas a convertirse en miembros. La relación administrador-miembro se establece cuando un potencial miembro acepta la invitación. Una cuenta de administrador CSPM de Security Hub puede administrar Security Hub CSPM para hasta 1000 cuentas de miembros por invitación.

Note

Si crea una organización basada en invitaciones en Security Hub CSPM, puede [pasar](#) posteriormente a utilizarla en su lugar. AWS Organizations Si tiene más de una cuenta de miembro, le recomendamos que utilice AWS Organizations en lugar de las invitaciones de CSPM de Security Hub para administrar sus cuentas de miembro. Para obtener información, consulte [Administrar Security Hub CSPM para varias cuentas con AWS Organizations](#).

La agregación entre regiones de resultados y otros datos están disponibles para las cuentas que invite a través del proceso de invitación manual. Sin embargo, el administrador debe invitar a la cuenta de miembro de la región de agregación y de todas las regiones vinculadas para que funcione la agregación entre regiones. Además, la cuenta de miembro debe tener el Security Hub CSPM activado en la región de agregación y en todas las regiones vinculadas para que el administrador pueda ver los resultados de la cuenta de miembro.

Las políticas de configuración no son compatibles con las cuentas miembros invitadas de forma manual. En su lugar, debe configurar los ajustes de CSPM de Security Hub por separado en cada cuenta de miembro y Región de AWS cuando utilice el proceso de invitación manual.

También debe utilizar el proceso manual basado en invitaciones para las cuentas que no pertenezcan a su organización. Por ejemplo, es posible que no incluya una cuenta de prueba en su organización. O bien, puede que desee consolidar cuentas de varias organizaciones en una sola cuenta de administrador CSPM de Security Hub. La cuenta de administrador CSPM de Security Hub debe enviar invitaciones a las cuentas que pertenezcan a otras organizaciones.

En la página de configuración de la consola CSPM de Security Hub, las cuentas que se agregaron mediante invitación aparecen en la pestaña Cuentas de invitación. Si utiliza la [configuración central](#), pero también invita a cuentas ajenas a su organización, puede ver los resultados de las cuentas basadas en invitaciones en esta pestaña. Sin embargo, el administrador de Security Hub CSPM no puede configurar cuentas basadas en invitaciones en todas las regiones mediante el uso de políticas de configuración.

En esta sección, se explica cómo administrar cuentas de miembros mediante invitaciones.

Temas

- [Añadir e invitar cuentas de miembros en Security Hub \(CSPM\)](#)
- [Responder a una invitación para ser miembro de Security Hub \(CSPM\)](#)
- [Desasociar las cuentas de los miembros en Security Hub \(CSPM\)](#)
- [Eliminar cuentas de miembros en Security Hub \(CSPM\)](#)
- [Desasociarse de una cuenta de administrador CSPM de Security Hub](#)
- [Transición a Organizations para gestionar las cuentas en Security Hub \(CSPM\)](#)

Añadir e invitar cuentas de miembros en Security Hub (CSPM)

Note

Recomendamos utilizar, AWS Organizations en lugar de Security Hub, invitaciones CSPM para gestionar las cuentas de los miembros. Para obtener información, consulte [Administrar Security Hub CSPM para varias cuentas con AWS Organizations](#).

Su cuenta pasa a ser la administradora de AWS Security Hub Cloud Security Posture Management (CSPM) para las cuentas que acepten su invitación para convertirse en una cuenta miembro de Security Hub CSPM.

Al aceptar una invitación de otra cuenta, su cuenta se convierte en cuenta de miembro, mientras que la otra cuenta se convierte en su administrador.

Si su cuenta es la cuenta de administrador, no podrá aceptar una invitación para convertirse en cuenta de miembro.

El proceso para agregar una cuenta de miembro consta de los siguientes pasos:

1. La cuenta de administrador agrega la cuenta de miembro a su lista.
2. La cuenta de administrador envía una invitación a la cuenta de miembro.
3. La cuenta de miembro acepta la invitación.

Adición de cuentas de miembro

Desde la consola CSPM de Security Hub, puede añadir cuentas a su lista de cuentas de miembros. En la consola CSPM de Security Hub, puede seleccionar las cuentas de forma individual o cargar un .csv archivo que contenga la información de la cuenta.

Para cada cuenta, debe proporcionar el ID de la cuenta y una dirección de correo electrónico. La dirección de correo electrónico debe ser la dirección de correo electrónico de contacto en caso de problemas de seguridad de la cuenta. No se utiliza para verificar la cuenta.

Elija el método que prefiera y siga estos pasos para agregar cuentas de miembro.

Security Hub CSPM console

Cómo agregar cuentas a su lista de cuentas de miembro

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>

Inicie sesión en las credenciales de una cuenta del administrador.

2. En el panel izquierdo, seleccione Configuración.
3. En la página Configuración, seleccione Cuentas, elija Agregar cuentas y, a continuación, realice alguna de las siguientes operaciones: A continuación, puede agregar cuentas de forma individual o cargar un archivo .csv que contenga la lista de cuentas.
4. Para seleccionar las cuentas, realice una de las operaciones siguientes:

- Para agregar las cuentas de una en una, debajo de Introducir cuentas escriba el ID y la dirección de correo electrónico de la cuenta que se va a agregar y, a continuación, elija Agregar.

Repita este proceso para cada cuenta.

- Para utilizar un archivo de valores separados por comas (.csv) para agregar varias cuentas, primero debe crear el archivo. El archivo debe contener el ID y la dirección de correo electrónico de cada cuenta que desee agregar.

En la lista .csv, las cuentas deben aparecer de una en una en cada línea. La primera línea del archivo .csv debe contener el encabezado. En el encabezado, la primera columna es **Account ID** y la segunda **Email**.

Cada una de las líneas siguientes debe contener un ID de cuenta y una dirección de correo electrónico válidos para la cuenta que se va a añadir.

Este es un ejemplo de un archivo .csv visto en un editor de texto.

```
Account ID,Email
111111111111,user@example.com
```

En un programa de hojas de cálculo, los campos aparecen en columnas independientes. El formato subyacente sigue separado por comas. Debe formatear la cuenta con números no IDs decimales. Por ejemplo, el ID de cuenta 444455556666 no puede tener el formato

444455556666.0. Asegúrese también de que el formato numérico no elimine ningún cero inicial del ID de la cuenta.

Para seleccionar el archivo, en la consola, seleccione Cargar lista (.csv). A continuación, seleccione Examinar.

Después de seleccionar el archivo, elija Agregar cuentas.

5. Cuando haya terminado de agregar cuentas, en Cuentas que se van a agregar, seleccione Siguiente.

Security Hub CSPM API

Agregación de cuentas a su lista de cuentas de miembro

Invoque la API [CreateMembers](#) desde la cuenta de administrador. Para añadir cada cuenta de miembro, debe proporcionar el Cuenta de AWS ID.

AWS CLI

Agregación de cuentas a su lista de cuentas de miembro

Ejecute el comando [create-members](#) desde la cuenta de administrador. Para añadir cada cuenta de miembro, debe proporcionar la Cuenta de AWS identificación.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

Ejemplo

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"}, {"AccountId": "123456789222"}]'
```

Cómo invitar cuentas de miembro

Una vez agregadas las cuentas de miembro, envíe una invitación a la cuenta de miembro. También puede volver a enviar una invitación a una cuenta que haya desvinculado del administrador.

Security Hub CSPM console

Invitación a potenciales cuentas de miembro

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>

Inicie sesión en las credenciales de una cuenta del administrador.

2. En el panel de navegación, elija Configuración y Cuentas.
3. En la cuenta que va a invitar, elija Invite (Invitar) en la columna Status (Estado).
4. Cuando se le pida confirmación, elija Invitar.

Note

Para volver a enviar invitaciones a cuentas desasociadas, seleccione cada una de las cuentas desasociadas en la página Cuentas. En Acciones, seleccione Volver a enviar invitación.

Security Hub CSPM API

Invitación a potenciales cuentas de miembro

Invoque la API [InviteMembers](#) desde la cuenta de administrador. Para cada cuenta a la que desee invitar, debe proporcionar el Cuenta de AWS ID.

AWS CLI

Invitación a potenciales cuentas de miembro

Ejecute el comando [invite-members](#) desde la cuenta de administrador. Para cada cuenta a la que quieras invitar, debes proporcionar el Cuenta de AWS ID.

```
aws securityhub invite-members --account-ids <accountIDs>
```

Ejemplo

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

Responder a una invitación para ser miembro de Security Hub (CSPM)

Note

Recomendamos utilizar, AWS Organizations en lugar de Security Hub, invitaciones CSPM para gestionar las cuentas de los miembros. Para obtener información, consulte [Administrar Security Hub CSPM para varias cuentas con AWS Organizations](#).

Puedes aceptar o rechazar una invitación para ser miembro de AWS Security Hub Cloud Security Posture Management (CSPM).

Si aceptas una invitación, tu cuenta se convierte en una cuenta de miembro de Security Hub CSPM. La cuenta que envió la invitación se convierte en su cuenta de administrador de CSPM de Security Hub. El usuario de la cuenta de administrador puede ver los resultados de su cuenta de miembro en Security Hub CSPM.

Si rechaza la invitación, su cuenta se marcará como Renunciada en la lista de cuentas de miembro de la cuenta de administrador.

Solo puede aceptar una invitación para ser miembro de la cuenta.

Para poder aceptar o rechazar una invitación, debe activar Security Hub CSPM.

Recuerde que todas las cuentas CSPM de Security Hub deben estar AWS Config habilitadas y configuradas para registrar todos los recursos. Para obtener más información sobre los requisitos AWS Config, consulte [Habilitar y configurar](#). AWS Config

Cómo aceptar una invitación

Puedes enviar una invitación para ser miembro de Security Hub CSPM desde la cuenta de administrador. A continuación, podrá aceptar la invitación tras iniciar sesión en la cuenta de miembro.

Elija el método que prefiera y siga los pasos para aceptar una invitación y convertirse en una cuenta de miembro.

Security Hub CSPM console

Aceptación de una invitación a una suscripción

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Configuración y Cuentas.
3. En la sección Cuenta de administrador, active Aceptar y, a continuación, seleccione Aceptar invitación.

Security Hub CSPM API

Aceptación de una invitación a una suscripción

Invoque la API [AcceptAdministratorInvitation](#). Debe proporcionar el identificador de la invitación y el Cuenta de AWS ID de la cuenta de administrador. Para recuperar los detalles de la invitación, utilice la operación [ListInvitations](#).

AWS CLI

Aceptación de una invitación a una suscripción

Ejecute el comando [accept-administrator-invitation](#). Debe proporcionar el identificador de la invitación y el Cuenta de AWS ID de la cuenta de administrador. Para recuperar los detalles de la invitación, ejecute el comando [list-invitations](#).

```
aws securityhub accept-administrator-invitation --administrator-id <administratorAccountID> --invitation-id <invitationID>
```

Ejemplo

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

Note

La consola CSPM de Security Hub sigue utilizándose. AcceptInvitation Con el tiempo, pasará a usar AcceptAdministratorInvitation. Cualquier política de IAM que controle

específicamente el acceso a esta función debe seguir empleando `AcceptInvitation`. También debe agregar `AcceptAdministratorInvitation` a sus políticas los permisos correctos una vez que la consola comience a utilizar `AcceptAdministratorInvitation`.

Cómo rechazar una invitación

Puedes rechazar una invitación para ser miembro de Security Hub CSPM. Cuando rechazas una invitación en la consola CSPM de Security Hub, tu cuenta se marca como Renunciada en la lista de cuentas de miembros de la cuenta de administrador. El estado Renunciado solo aparece al iniciar sesión en la consola CSPM de Security Hub con la cuenta de administrador. Sin embargo, no habrá cambios en la invitación en la consola de la cuenta de miembro hasta que inicie sesión en la cuenta de administrador y elimine la invitación.

Para rechazar una invitación, debe iniciar sesión en la cuenta de miembro que recibió la invitación.

Elija el método preferido y siga los pasos para rechazar una invitación para ser una cuenta de miembro.

Security Hub CSPM console

Rechazo de una invitación a una membresía

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Configuración y Cuentas.
3. En la sección Cuenta de administrador, seleccione Rechazar la invitación.

Security Hub CSPM API

Rechazo de una invitación a una membresía

invoque la API [DeclineInvitations](#). Debe proporcionar el Cuenta de AWS ID de la cuenta de administrador que emitió la invitación. Para ver la información sobre sus invitaciones, utilice la operación [ListInvitations](#).

AWS CLI

Rechazo de una invitación a una membresía

Ejecute el comando [decline-invitations](#). Debe proporcionar el Cuenta de AWS ID de la cuenta de administrador que emitió la invitación. Para ver la información sobre sus invitaciones, ejecute el comando [list-invitations](#).

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

Ejemplo

```
aws securityhub decline-invitations --account-ids "123456789012"
```

Desasociar las cuentas de los miembros en Security Hub (CSPM)

Note

Recomendamos utilizar, AWS Organizations en lugar de Security Hub, invitaciones CSPM para gestionar las cuentas de los miembros. Para obtener información, consulte [Administrar Security Hub CSPM para varias cuentas con AWS Organizations](#).

Una cuenta de administrador de AWS Security Hub Cloud Security Posture Management (CSPM) puede desasociar una cuenta de miembro para dejar de recibir y ver los resultados de esa cuenta. Debe desvincular una cuenta de miembro antes de poder eliminarla.

Al desvincular una cuenta de miembro, permanece en la lista de cuentas de miembro con el estado Eliminada (desvinculada). Su cuenta se elimina de la información de la cuenta de administrador de la cuenta de miembro.

Para volver a recibir los resultados de la cuenta, puede volver a enviar la invitación. Para eliminar la cuenta de miembro por completo, puede eliminarla.

Elija el método que prefiera y siga los pasos para desasociar una cuenta de miembro invitada manualmente desde la cuenta de administrador.

Security Hub CSPM console

Desasociación de una cuenta de miembro invitada manualmente

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>

Inicie sesión en las credenciales de una cuenta del administrador.

2. En el panel de navegación, en Configuración, elija Configuración.
3. En la sección Cuentas, seleccione las cuentas que desee desasociar.
4. Seleccione Acciones y, a continuación, Desasociar cuenta.

Security Hub CSPM API

Desasociación de una cuenta de miembro invitada manualmente

Invoque la API [DisassociateMembers](#) desde la cuenta de administrador. Debe proporcionar las cuentas Cuenta de AWS IDs de los miembros que desee desvincular. Para ver una lista de las cuentas miembro, utilice la operación [ListMembers](#).

AWS CLI

Desasociación de una cuenta de miembro invitada manualmente

Ejecute el comando [disassociate-members](#) desde la cuenta de administrador. Debe proporcionar las cuentas Cuenta de AWS IDs de los miembros que desee desasociar. Para ver una lista de las cuentas de miembro, ejecute el comando [list-members](#).

```
aws securityhub disassociate-members --account-ids <accountIds>
```

Ejemplo

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Eliminar cuentas de miembros en Security Hub (CSPM)

Note

Recomendamos utilizar, AWS Organizations en lugar de Security Hub, invitaciones CSPM para gestionar las cuentas de los miembros. Para obtener información, consulte [Administrar Security Hub CSPM para varias cuentas con AWS Organizations](#).

Como cuenta de administrador de AWS Security Hub Cloud Security Posture Management (CSPM), puede eliminar las cuentas de los miembros que se agregaron por invitación. Antes de poder eliminar una cuenta habilitada, debe desvincularla.

Al eliminar una cuenta de miembro, se elimina por completo de la lista. Para restaurar la suscripción de la cuenta, debe agregarla e invitarla de nuevo, como si se tratara de una cuenta de miembro completamente nueva.

No puede eliminar las cuentas que pertenezcan a una organización y que se administren mediante la integración con. AWS Organizations

Elija el método que prefiera y siga los pasos para eliminar las cuentas de miembro invitados manualmente.

Security Hub CSPM console

Eliminación de una cuenta de miembro invitada manualmente

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>

Inicie sesión con la cuenta de administrador.
2. En el panel de navegación, elija Configuración y, a continuación, elija Configuración.
3. Seleccione la pestaña Cuentas de invitación. A continuación, seleccione las cuentas que desea eliminar.
4. Elija Acciones y, a continuación, elija Eliminar. Esta opción solo está disponible si ha desasociado la cuenta. Debe desasociar una cuenta de miembro antes de poder eliminarla.

Security Hub CSPM API

Eliminación de una cuenta de miembro invitada manualmente

Invoque la API [DeleteMembers](#) desde la cuenta de administrador. Debe proporcionar las cuentas de AWS IDs de los miembros que desea eliminar. Para recuperar la lista de cuentas de miembro, invoque la API [ListMembers](#).

AWS CLI

Eliminación de una cuenta de miembro invitada manualmente

Ejecute el comando [delete-members](#) desde la cuenta de administrador. Debe proporcionar las cuentas Cuenta de AWS IDs de los miembros que desea eliminar. Para recuperar la lista de cuentas de miembro, ejecute el comando [list-members](#).

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

Ejemplo

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

Desasociarse de una cuenta de administrador CSPM de Security Hub

Note

Recomendamos utilizar, AWS Organizations en lugar de Security Hub, invitaciones CSPM para gestionar las cuentas de los miembros. Para obtener información, consulte [Administrar Security Hub CSPM para varias cuentas con AWS Organizations](#).

Si su cuenta se agregó como cuenta de miembro de AWS Security Hub Cloud Security Posture Management (CSPM) por invitación, puede desasociar la cuenta de miembro de la cuenta de administrador. Tras desasociar una cuenta de miembro, Security Hub CSPM no envía los resultados de la cuenta a la cuenta de administrador.

Las cuentas de los miembros que se administran mediante la integración con no AWS Organizations pueden disociar sus cuentas de la cuenta de administrador. Solo el administrador delegado de CSPM de Security Hub puede desasociar las cuentas de los miembros que se administran con Organizations.

Cuando se desvincula de su cuenta de administrador, su cuenta permanece en la lista de miembros de la cuenta de administrador con el estado Renunciado. Sin embargo, la cuenta de administrador no recibe ningún dato sobre su cuenta.

Tras desasociarse de la cuenta de administrador, la invitación para ser miembro seguirá vigente. Puede volver a aceptar la invitación en el futuro.

Security Hub CSPM console

Cómo desvincularse de su cuenta de administrador

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Configuración y Cuentas.
3. En la sección Cuenta de administrador, desactive Aceptar y, a continuación, seleccione Actualizar.

Security Hub CSPM API

Desasociación de su cuenta de administrador

invoque la API [DisassociateFromAdministratorAccount](#).

AWS CLI

Desasociación de su cuenta de administrador

Ejecute el comando [disassociate-from-administrator-account](#).

```
aws securityhub disassociate-from-administrator-account
```

Note

La consola CSPM de Security Hub sigue utilizándose.

`DisassociateFromMasterAccount` Con el tiempo, pasará a usar `DisassociateFromAdministratorAccount`. Cualquier política de IAM que controle específicamente el acceso a esta función debe seguir empleando `DisassociateFromMasterAccount`. También debe agregar `DisassociateFromAdministratorAccount` a sus políticas los permisos correctos una vez que la consola comience a utilizar `DisassociateFromAdministratorAccount`.

Transición a Organizations para gestionar las cuentas en Security Hub (CSPM)

Al gestionar las cuentas manualmente en AWS Security Hub Cloud Security Posture Management (CSPM), debe invitar a posibles cuentas de miembros y configurar cada cuenta de miembro por separado en cada una de ellas. Región de AWS

Al integrar Security Hub CSPM AWS Organizations, puede eliminar la necesidad de enviar invitaciones y obtener un mayor control sobre cómo se configura y personaliza Security Hub CSPM en su organización. Por este motivo, le recomendamos que utilice AWS Organizations en lugar de las invitaciones CSPM de Security Hub para gestionar las cuentas de los miembros. Para obtener información, consulte [Administrar Security Hub CSPM para varias cuentas con AWS Organizations](#).

Es posible utilizar un enfoque combinado en el que se utiliza la AWS Organizations integración, pero también se pueden invitar manualmente a cuentas ajenas a la organización. Sin embargo, recomendamos utilizar exclusivamente la integración de Organizations. [La configuración central](#), una función que le ayuda a gestionar el CSPM de Security Hub en varias cuentas y regiones, solo está disponible cuando se integra con Organizations.

En esta sección, se explica cómo pasar de la administración manual de cuentas basada en invitaciones a la administración de cuentas con AWS Organizations.

Integración de Security Hub CSPM con AWS Organizations

En primer lugar, debe integrar Security Hub CSPM y. AWS Organizations

Siga los pasos que se indican a continuación para integrar estos servicios:

- Creación de una organización en AWS Organizations. Para obtener instrucciones sobre cómo hacerlo, consulte [Creación de una organización](#) en la Guía del usuario de AWS Organizations .
- Desde la cuenta de administración de Organizations, designe una cuenta de administrador delegado CSPM de Security Hub.

Note

La cuenta de administración de Organizations no se puede establecer como cuenta de administrador delegado.

Para obtener instrucciones detalladas, consulta [Integración de Security Hub CSPM con AWS Organizations](#).

Al completar los pasos anteriores, se concede un [acceso de confianza](#) para el Security Hub CSPM en AWS Organizations. Esto también habilita el CSPM de Security Hub en la cuenta actual. Región de AWS de administrador delegado.

El administrador delegado puede gestionar la organización en Security Hub CSPM, principalmente añadiendo las cuentas de la organización como cuentas de miembros de Security Hub CSPM. El administrador también puede acceder a determinadas configuraciones, datos y recursos de CSPM de Security Hub para esas cuentas.

Al realizar la transición a la administración de cuentas mediante Organizations, las cuentas basadas en invitaciones no se convierten automáticamente en miembros de Security Hub CSPM. Solo las cuentas que añada a su nueva organización pueden convertirse en miembros de Security Hub CSPM.

Tras activar la integración, puede administrar las cuentas con Organizations. Para obtener información, consulte [Administrar Security Hub CSPM para varias cuentas con AWS Organizations](#). La administración de cuentas varía en función del tipo de configuración de la organización.

Acciones permitidas por parte del administrador y las cuentas de los miembros en Security Hub (CSPM)

Las cuentas de administrador y miembro tienen acceso a las acciones de AWS Security Hub Cloud Security Posture Management (CSPM) que se indican en las siguientes tablas. En las tablas, los valores tienen los siguientes significados:

- Cualquiera: la cuenta puede llevar a cabo la acción para todas las cuentas de miembro del mismo administrador.
- Actual: la cuenta solo puede llevar a cabo la acción por sí misma (la cuenta en la que ha iniciado sesión).
- Guion: indica que la cuenta no puede llevar a cabo la acción.

Como se indica en las tablas, las acciones permitidas varían según el tipo de configuración que utilice la organización AWS Organizations y el tipo de configuración que utilice. Para obtener más información acerca de la diferencia la configuración local y centralizada, consulte [Administrar cuentas con AWS Organizations](#).

Security Hub CSPM no copia los resultados de las cuentas de los miembros en la cuenta de administrador. En Security Hub CSPM, todos los hallazgos se incorporan a una región específica para una cuenta específica. En cada región, la cuenta del administrador puede ver y gestionar los resultados de sus cuentas de miembro en esa región.

Si establece una región de agregación, la cuenta de administrador puede ver y administrar los resultados de las cuentas de miembro de las regiones vinculadas que se replican en la región de agregación. Para obtener más información sobre la agregación entre regiones, consulte [Agregación entre regiones](#).

En las siguientes tablas se especifican los permisos predeterminados para las cuentas de administrador y miembro. Puede usar políticas de IAM personalizadas para restringir aún más el acceso a las características y funciones de CSPM de Security Hub. Para obtener orientación y ejemplos, consulte la entrada del blog [Alineación de las políticas de IAM con las personas de los usuarios para AWS Security Hub Cloud Security Posture Management \(CSPM\)](#).

Acciones permitidas si integra con Organizations y usa la configuración centralizada

Las cuentas de administrador y miembro pueden acceder a las acciones de CSPM de Security Hub de la siguiente manera si se integra con Organizations y usa la configuración central.

Acción	Cuenta de administrador delegado CSPM de Security Hub	Cuenta de miembro administrada de forma centralizada	Cuenta de miembro autoadministrada
Cree y gestione las políticas de configuración de Security Hub (CSPM)	Para cuentas administradas automáticamente y de forma centralizada	–	–
Visualización de cuentas de la organización	Cualquiera	–	–
Desvincular cuenta de miembro	Cualquiera	–	–

Acción	Cuenta de administrador delegado CSPM de Security Hub	Cuenta de miembro administrada de forma centralizada	Cuenta de miembro autoadministrada
Eliminar cuenta de miembro	Cualquier cuenta que no sea de una organización	–	–
Desactivar Security Hub (CSPM)	Para cuentas actuales y cuentas administradas de forma centralizada	–	Actuales (deben desasociarse de la cuenta de administrador)
Vea los resultados y el historial de búsquedas	Cualquiera	Actuales	Actuales
Actualizar los resultados	Cualquiera	Actuales	Actuales
Ver los resultados de los hallazgos	Cualquiera	Actuales	Actuales
Ver los detalles de control	Cualquiera	Actuales	Actuales
Activación o desactivación de los resultados de control consolidados	Cualquiera	–	–
Habilitar y deshabilitar estándares	Para cuentas actuales y cuentas administradas de forma centralizada	–	Actuales

Acción	Cuenta de administrador delegado CSPM de Security Hub	Cuenta de miembro administrada de forma centralizada	Cuenta de miembro autoadministrada
Habilitar y deshabilitar controles	Para cuentas actuales y cuentas administradas de forma centralizada	–	Actuales
Habilitar y deshabilitar integraciones	Actuales	Actuales	Actuales
Configurar agregación entre regiones	Cualquiera	–	–
Selección de la región de origen y las regiones vinculadas	Cualquiera (debe detener y reiniciar la configuración centralizada para cambiar la región de origen)	–	–
Configurar acciones personalizadas	Actuales	Actuales	Actuales
Configurar reglas de automatización	Cualquiera	–	–
Configurar hallazgos personalizados	Actuales	Actuales	Actuales

Acciones permitidas si integra con Organizations y usa la configuración local

Las cuentas de administrador y miembro pueden acceder a las acciones de CSPM de Security Hub de la siguiente manera si se integra con Organizations y usa la configuración local.

Acción	Cuenta de administrador delegado CSPM de Security Hub	Cuenta de miembro
Cree y gestione las políticas de configuración de Security Hub (CSPM)	–	–
Visualización de cuentas de la organización	Cualquiera	–
Desvincular cuenta de miembro	Cualquiera	–
Eliminar cuenta de miembro	–	–
Desactivar Security Hub (CSPM)	–	Actual (si la cuenta está desasociada del administrador delegado)
Vea los resultados y el historial de búsquedas	Cualquiera	Actuales
Actualizar los resultados	Cualquiera	Actuales
Ver los resultados de los hallazgos	Cualquiera	Actuales
Ver los detalles de control	Cualquiera	Actuales
Activación o desactivación de los resultados de control consolidados	Cualquiera	–
Habilitar y deshabilitar estándares	Actuales	Actuales
Habilite automáticamente el Security Hub, el CSPM y los estándares predeterminados	Para cuentas actuales y cuentas nuevas de la organización	–

Acción	Cuenta de administrador delegado CSPM de Security Hub	Cuenta de miembro
en las nuevas cuentas de la organización		
Habilitar y deshabilitar controles	Actuales	Actuales
Habilitar y deshabilitar integraciones	Actuales	Actuales
Configurar agregación entre regiones	Cualquiera	–
Configurar acciones personalizadas	Actuales	Actuales
Configurar reglas de automatización	Cualquiera	–
Configurar hallazgos personalizados	Actuales	Actuales

Acciones permitidas para las cuentas basadas en invitaciones

Las cuentas de administrador y miembro pueden acceder a las acciones de CSPM de Security Hub de la siguiente manera si utiliza el método basado en invitaciones para administrar las cuentas manualmente en lugar de integrarlas con AWS Organizations

Acción	Cuenta de administrador CSPM de Security Hub	Cuenta de miembro
Cree y gestione las políticas de configuración de Security Hub (CSPM)	–	–

Acción	Cuenta de administrador CSPM de Security Hub	Cuenta de miembro
Visualización de cuentas de la organización	Cualquiera	–
Desvincular cuenta de miembro	Cualquiera	Actuales
Eliminar cuenta de miembro	Cualquiera	–
Desactivar Security Hub (CSPM)	Actual (si no hay cuentas de miembro habilitadas)	Actual (si la cuenta está desasociada de la cuenta de administrador)
Vea los resultados y el historial de búsquedas	Cualquiera	Actuales
Actualizar los resultados	Cualquiera	Actuales
Ver los resultados de los hallazgos	Cualquiera	Actuales
Ver los detalles de control	Cualquiera	Actuales
Activación o desactivación de los resultados de control consolidados	Cualquiera	–
Habilitar y deshabilitar estándares	Actuales	Actuales
Habilite automáticamente el Security Hub, el CSPM y los estándares predeterminados en las nuevas cuentas de la organización	–	–

Acción	Cuenta de administrador CSPM de Security Hub	Cuenta de miembro
Habilitar y deshabilitar controles	Actuales	Actuales
Habilitar y deshabilitar integraciones	Actuales	Actuales
Configurar agregación entre regiones	Cualquiera	–
Configurar acciones personalizadas	Actuales	Actuales
Configurar reglas de automatización	Cualquiera	–
Configurar hallazgos personalizados	Actuales	Actuales

Efecto de las acciones de la cuenta en los datos de CSPM de Security Hub

Estas acciones de la cuenta tienen los siguientes efectos en los AWS datos de Security Hub Cloud Security Posture Management (CSPM).

Security Hub (CSPM) desactivado

Si utiliza la [configuración central](#), el administrador delegado (DA) puede crear políticas de configuración de CSPM del Security Hub que inhabiliten la gestión de la postura de AWS seguridad (CSPM) de Security Hub Cloud en cuentas y unidades organizativas específicas (OU). En este caso, el CSPM de Security Hub está deshabilitado en las cuentas especificadas y OUs en tu región de origen y en cualquier región vinculada. Si no utiliza la configuración central, debe deshabilitar el CSPM de Security Hub por separado en cada cuenta y región en la que lo haya activado. No puede usar la configuración central si el CSPM de Security Hub está deshabilitado en la cuenta DA.

No se generan resultados para la cuenta de administrador si Security Hub CSPM está deshabilitado en la cuenta de administrador. Los hallazgos archivados existentes se eliminan después de 30 días. Los hallazgos activos existentes se eliminan después de 90 días.

Servicios de AWS Se eliminan las integraciones con otras.

Los estándares de seguridad y controles habilitados se deshabilitan.

Otros datos y configuraciones de CSPM de Security Hub, incluidas las acciones personalizadas, la información y las suscripciones a productos de terceros, se conservan durante 90 días.

Cuenta miembro disociada de la cuenta de administrador

Cuando una cuenta miembro se desvincula de la cuenta de administrador, esta pierde el permiso para ver los resultados en la cuenta de miembro. Sin embargo, el CSPM de Security Hub sigue activado en ambas cuentas.

Si usa la configuración central, el DA no puede configurar el CSPM de Security Hub para una cuenta de miembro que esté disociada de la cuenta DA.

La configuración personalizada o las integraciones definidas para la cuenta de administrador no se aplican a los resultados de la antigua cuenta de miembro. Por ejemplo, después de disociar las cuentas, es posible que tengas una acción personalizada en la cuenta de administrador utilizada como patrón de eventos en una EventBridge regla de Amazon. Sin embargo, esta acción personalizada no se puede utilizar en la cuenta de miembro.

En la lista de cuentas de la cuenta de administrador de CSPM de Security Hub, una cuenta eliminada tiene el estado Desasociada.

Cómo eliminar una cuenta miembro de una organización

Cuando se elimina una cuenta de miembro de una organización, la cuenta de administrador de CSPM de Security Hub pierde el permiso para ver los resultados de la cuenta de miembro. Sin embargo, el CSPM de Security Hub sigue activado en ambas cuentas con la misma configuración que tenían antes de la eliminación.

Si utiliza la configuración central, no podrá configurar el CSPM de Security Hub para una cuenta de miembro una vez que se haya eliminado de la organización a la que pertenece el administrador delegado. Sin embargo, la cuenta retiene la configuración que tenía antes de la eliminación, a menos que la cambie manualmente.

En la lista de cuentas de la cuenta de administrador de CSPM de Security Hub, una cuenta eliminada tiene el estado Eliminada.

Cuenta suspendida

Cuando Cuenta de AWS se suspende una, la cuenta pierde el permiso para ver sus hallazgos en Security Hub CSPM. No se generan resultados para esa cuenta. La cuenta de administrador de una cuenta suspendida puede ver los hallazgos existentes sobre la cuenta.

En el caso de una cuenta de organización, el estado de la cuenta de miembro también puede cambiar a Cuenta suspendida. Esto sucede si la cuenta se suspende en el mismo momento en que la cuenta del administrador intenta habilitarla. La cuenta de administrador de una Cuenta suspendida no puede ver los resultados de esa cuenta. De lo contrario, el estado suspendido no afectará al estado de la cuenta miembro.

Si utiliza la configuración centralizada, se producirá un error en la asociación de políticas si el administrador delegado intenta asociar una política de configuración a una cuenta suspendida.

Transcurridos 90 días, la cuenta se termina o se reactiva. Cuando se reactiva la cuenta, se restauran los permisos CSPM de Security Hub. Si el estado de la cuenta de miembro es Cuenta suspendida, la cuenta del administrador debe habilitar la cuenta manualmente.

Cuenta cerrada

Cuando un Cuenta de AWS está cerrado, el Security Hub CSPM responde al cierre de la siguiente manera.

Si la cuenta es una cuenta de administrador CSPM de Security Hub, se elimina como cuenta de administrador y se eliminan todas las cuentas de los miembros. Si la cuenta es una cuenta de miembro, se disocia y se elimina como miembro de la cuenta de administrador CSPM de Security Hub.

Security Hub CSPM conserva las conclusiones archivadas existentes en la cuenta durante 30 días. En el caso de una constatación de control, el cálculo de 30 días se basa en el valor del UpdatedAt campo de la constatación. Para otro tipo de hallazgo, el cálculo se basa en el valor del ProcessedAt campo UpdatedAt o del hallazgo, sea cual sea la fecha más reciente. Al final de este período de 30 días, Security Hub CSPM elimina permanentemente el hallazgo de la cuenta.

Security Hub CSPM conserva los hallazgos activos existentes en la cuenta durante 90 días. En el caso de una constatación de control, el cálculo de 90 días se basa en el valor del UpdatedAt campo

de la constatación. Para otro tipo de hallazgo, el cálculo se basa en el valor del ProcessedAt campo UpdatedAt o del hallazgo, sea cual sea la fecha más reciente. Al final de este período de 90 días, Security Hub CSPM elimina permanentemente el hallazgo de la cuenta.

Para conservar los hallazgos existentes a más largo plazo, puede exportarlos a un bucket de S3. Puedes hacerlo mediante una acción personalizada con una EventBridge regla de Amazon. Para obtener más información, consulte [Uso EventBridge para respuesta y remediación automatizadas](#).

 Important

En el caso de los clientes registrados AWS GovCloud (US) Regions, haz una copia de seguridad de los datos de tu póliza y otros recursos de la cuenta y los borra antes de cerrarla. No tendrás acceso a los recursos ni a los datos después de cerrar la cuenta.

Para obtener más información, consulta [Cerrar una Cuenta de AWS](#) en la guía de AWS Account Management referencia.

Descripción de la agregación entre regiones en Security Hub CSPM

Note

La región de agregación ahora se denomina región de origen. Algunas operaciones de la API CSPM de Security Hub siguen utilizando el antiguo término Región de agregación.

Al utilizar la agregación entre regiones en AWS Security Hub Cloud Security Posture Management (CSPM), puede agregar hallazgos, encontrar actualizaciones, información, controlar los estados de cumplimiento y los puntajes de seguridad de varias regiones de origen Regiones de AWS a una sola. A continuación, puede administrar todos estos datos desde la región de origen.

Supongamos que establece este de EE. UU. (norte de Virginia) como región de origen y oeste de EE. UU. (Oregón) y oeste de EE. UU. (norte de California) como regiones vinculadas. Al ver la página Resultados en Este de EE. UU. (Norte de Virginia), verá los resultados de las tres regiones. Las actualizaciones de esos resultados también se reflejan en las tres regiones.

Note

En AWS GovCloud (US), la agregación entre regiones solo se admite para los hallazgos, las actualizaciones y la información de todos los países. AWS GovCloud (US) En concreto, solo puede agregar los hallazgos, las actualizaciones y los conocimientos entre AWS GovCloud (EE. UU. este) y (EE. UU., oeste). AWS GovCloud En las regiones de China, solo se admite agregación entre regiones de los resultados, las actualizaciones de resultados y los hallazgos de las regiones de China. En concreto, solo puede agregar resultados, actualizaciones de resultados y hallazgos entre China (Pekín) y China (Ningxia).

Si un control está activado en una región vinculada pero deshabilitado en la región de origen, podrá ver el estado de conformidad del control desde la región de origen, pero no podrá habilitar ni deshabilitar ese control desde la región de origen. La única excepción es si se utiliza la [configuración centralizada](#). Si utiliza la configuración central, el administrador CSPM de Security Hub delegado puede configurar los controles en la región de origen y en las regiones vinculadas desde la región de origen.

Si ha establecido una región de origen, las [puntuaciones de seguridad](#) tienen en cuenta los estados de control en todas las regiones vinculadas. Para ver las puntuaciones de seguridad y los estados de cumplimiento entre regiones, añada los siguientes permisos a su función de IAM que utiliza Security Hub CSPM:

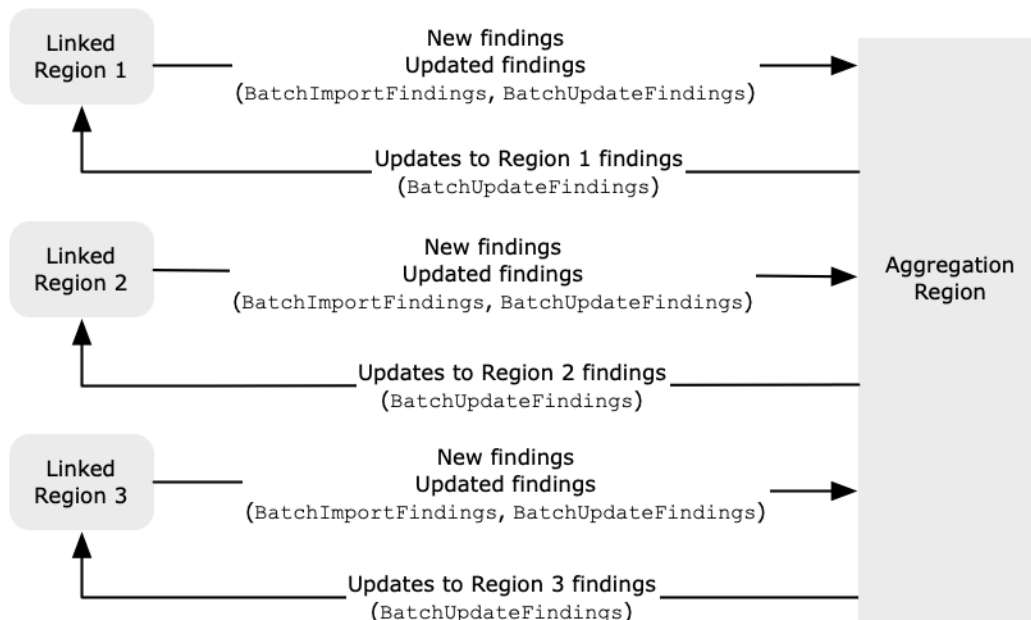
- [ListSecurityControlDefinitions](#)
- [BatchGetStandardsControlAssociations](#)
- [BatchUpdateStandardsControlAssociations](#)

Tipos de datos que se agregan

Cuando la agregación entre regiones está habilitada con una o más regiones vinculadas, Security Hub CSPM replica los siguientes datos de las regiones vinculadas a la región de origen. Esto ocurre en todas las cuentas que tienen habilitada la agregación entre regiones.

- Resultados
- Información
- Estados de control de la conformidad
- Puntuaciones de seguridad

Además de los nuevos datos de la lista anterior, Security Hub CSPM también replica las actualizaciones de estos datos entre las regiones vinculadas y la región de origen. Las actualizaciones que se producen en una región vinculada se replican en la región de origen. Las actualizaciones que se producen en la región de origen se replican de vuelta en la región vinculada. Si hay actualizaciones contradictorias en la región de origen y en la región vinculada, se utiliza la actualización más reciente.



La agregación entre regiones no aumenta el costo del Security Hub CSPM. No se le cobrará nada cuando Security Hub CSPM replique nuevos datos o actualizaciones.

En la región de origen, la página Resumen ofrece una vista de los resultados activos en las regiones vinculadas. Para más información, consulte [Visualización de un resumen de los resultados entre regiones por gravedad](#). Otros paneles de la página Resumen que analizan los resultados también muestran información de todas las regiones vinculadas.

Las puntuaciones de seguridad en la región de origen se calculan comparando el número de controles aprobados con el número de controles habilitados en todas las regiones vinculadas. Además, si un control está activado en al menos una región vinculada, estará visible en las páginas de detalles de las normas de seguridad de la región de origen. El estado de cumplimiento de los controles en las páginas de detalles de las normas refleja los resultados de las regiones vinculadas. Si un control de seguridad asociado a un control falla en una o más regiones vinculadas, el estado de conformidad de ese control aparece como Con fallos en las páginas de detalles de las normas de la región de origen. El número de controles de seguridad incluye los resultados de todas las regiones vinculadas.

El CSPM de Security Hub solo agrega datos de las regiones en las que una cuenta tiene activado el CSPM de Security Hub. El CSPM de Security Hub no se habilita automáticamente para una cuenta en función de la configuración de agregación entre regiones.

Es posible activar la agregación entre regiones sin seleccionar ninguna región vinculada. En este caso, no se replican los datos.

Agregación de cuentas de administrador y de miembros

La agregación entre regiones se configura mediante cuentas independientes, cuentas de miembros y cuentas de administrador. Si un administrador realiza la configuración, la presencia de la cuenta de administrador es esencial para que la agregación entre regiones funcione en las cuentas administradas. Si la cuenta de administrador se elimina o se desvincula de una cuenta de miembro, se detiene la agregación entre regiones para la cuenta de miembro. Esto se cumple incluso si la cuenta tenía activada la agregación entre regiones antes de que se iniciara la asociación administrador-miembro.

Cuando una cuenta de administrador habilita la agregación entre regiones, Security Hub CSPM replica los datos que la cuenta de administrador genera en todas las regiones vinculadas a la región de origen. Además, Security Hub CSPM identifica las cuentas de los miembros que están asociadas a ese administrador y cada cuenta de miembro hereda la configuración de agregación entre regiones del administrador. Security Hub CSPM replica los datos que genera una cuenta de miembro en todas las regiones vinculadas a la región de origen.

El administrador puede acceder a los resultados de seguridad y administrarlos desde todas las cuentas de miembros de las regiones administradas. Sin embargo, como administrador de CSPM de Security Hub, debe iniciar sesión en la región de origen para ver los datos agregados de todas las cuentas de los miembros y las regiones vinculadas.

Como cuenta de miembro de Security Hub CSPM, debe iniciar sesión en la región de origen para ver los datos agregados de su cuenta de todas las regiones vinculadas. Las cuentas de miembros no tienen permisos para ver los datos de otras cuentas de miembros.

Una cuenta de administrador puede invitar manualmente a las cuentas de los miembros o actuar como administradora delegada de una organización con la que esté integrada. AWS Organizations En el caso de una [cuenta de miembro invitada de forma manual](#), el administrador debe invitar a la cuenta de la región de origen y de todas las regiones vinculadas para que la agregación entre regiones funcione. Además, la cuenta del miembro debe tener el Security Hub CSPM activado en la región de origen y en todas las regiones vinculadas para que el administrador pueda ver los resultados de la cuenta del miembro. Si no utilizas la región de origen para otros fines, puedes deshabilitar las integraciones y los estándares CSPM de Security Hub en esa región para evitar cargos.

Si tiene pensado utilizar la agregación entre regiones y posee varias cuentas de administrador, se recomienda que siga estas prácticas:

- Cada cuenta de administrador tiene cuentas de miembro diferentes.
- Cada cuenta de administrador tiene las mismas cuentas de miembro en todas las regiones.
- Cada cuenta de administrador utiliza una región de origen diferente.

 Note

Para entender el impacto de la agregación entre regiones en la configuración centralizada, consulte [Impacto de la configuración centralizada en la agregación entre regiones](#).

Impacto de la configuración centralizada en la agregación entre regiones

La configuración central es una función opcional de AWS Security Hub Cloud Security Posture Management (CSPM) que puede utilizar si se integra con ella. AWS Organizations Si utiliza la configuración central, la cuenta de administrador delegado puede configurar el servicio CSPM, los estándares y los controles de Security Hub para las cuentas y las unidades organizativas (OU) de la organización. Para configurar las cuentas OUs, el administrador delegado crea políticas de configuración CSPM de Security Hub. Las políticas de configuración se pueden usar para definir si el CSPM de Security Hub está habilitado o deshabilitado y qué estándares y controles están habilitados. El administrador delegado asocia las políticas de configuración a cuentas específicas o a la raíz (toda la organización). OUs

El administrador delegado puede crear y administrar políticas de configuración para la organización solo desde la región de origen. Además, las políticas de configuración entran en vigor en la región de origen y en todas las regiones vinculadas. No puede crear una política de configuración que se aplique exclusivamente a algunas regiones vinculadas. Para obtener información sobre la agregación entre regiones, consulte [Agregación entre regiones](#).

Para utilizar la configuración centralizada, debe designar una región de origen. Si lo desea, puede elegir una o más regiones como regiones vinculadas. También puede optar por designar una región de origen sin ninguna región vinculada.

Cambiar la configuración de la agregación entre regiones puede afectar a las políticas de configuración. Al agregar una región vinculada, las políticas de configuración se aplican en esa región. Si la región es una [región opcional](#), debe estar habilitada para que las políticas de

configuración se apliquen allí. Por el contrario, al eliminar una región vinculada, las políticas de configuración dejan de tener efecto en esa región. En esa región, las cuentas mantienen la configuración que tenían cuando se eliminó la región vinculada. Puede cambiar esa configuración, pero debe hacerlo por separado en cada cuenta y región.

Si elimina o cambia la región de origen, se eliminarán las políticas de configuración y las asociaciones de políticas. Ya no podrá utilizar la configuración centralizada ni crear políticas de configuración en ninguna región. Las cuentas mantienen la configuración que tenían antes de que se cambiara o eliminara la región de origen. Puede cambiar esa configuración en cualquier momento, pero, como ya no utiliza la configuración centralizada, la configuración debe modificarse por separado en cada cuenta y región. Puede utilizar la configuración centralizada y volver a crear políticas de configuración si designa una nueva región de origen.

Para obtener más información acerca de la configuración centralizada, consulte [Descripción de la configuración central en Security Hub \(CSPM\)](#).

Habilitación de agregación entre regiones

Note

La región de agregación ahora se denomina región de origen. Algunas operaciones de la API CSPM de Security Hub siguen utilizando el antiguo término Región de agregación.

Debe habilitar la agregación entre regiones desde la región Región de AWS que desee designar como región de origen.

Para habilitar la agregación entre regiones, debe crear un recurso CSPM de Security Hub denominado agregador de búsquedas. El recurso del agregador de resultados especifica su región de origen y las regiones vinculadas (si las hubiera).

No puede usar una región Región de AWS que esté deshabilitada de forma predeterminada como región de origen. Para obtener una lista de regiones que están deshabilitadas de forma predeterminada, consulte [Habilitar una región](#) en la Referencia general de AWS.

Cuando activa la agregación entre regiones, puede especificar una o más regiones vinculadas si lo desea. También puede elegir si desea vincular automáticamente las nuevas regiones cuando Security Hub CSPM comience a admitirlas y haya optado por ellas.

Security Hub CSPM console

Cómo habilitar la agregación entre regiones

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
2. Con el Región de AWS selector, inicie sesión en la región que desee usar como región de agregación.
3. En el menú de navegación CSPM de Security Hub, seleccione Configuración y, a continuación, Regiones.
4. En Agregación de resultados, elija Configuración de la agregación de resultados.

De forma predeterminada, la región de origen aparece como Sin región de agregación.

5. En Región de agregación, seleccione la opción para designar la región actual como región de origen.
6. De forma opcional, en Regiones vinculadas, seleccione las regiones desde las que desea agregar datos.
7. Para agregar automáticamente los datos de las nuevas regiones de la partición, tal como las admite Security Hub CSPM y usted opta por ellas, seleccione Vincular futuras regiones.
8. Seleccione Save.

Security Hub CSPM API

Desde la región que desee utilizar como región de origen, utilice la [CreateFindingAggregator](#) operación de la API CSPM de Security Hub. Si usa la AWS CLI, ejecute el [create-finding-aggregator](#) comando.

En `RegionLinkingMode`, elija una de las siguientes opciones:

- **ALL_REGIONS**— Security Hub CSPM agrega datos de todas las regiones. Security Hub CSPM también agrega datos de nuevas regiones a medida que son compatibles y usted opta por ellas.
- **ALL_REGIONS_EXCEPT_SPECIFIED**— Security Hub CSPM agrega datos de todas las regiones, excepto de las regiones que desee excluir. Security Hub CSPM también agrega datos de nuevas regiones a medida que son compatibles y usted opta por ellas. Utilice `Regions` para proporcionar la lista de regiones que se van a excluir de la agregación.

- **SPECIFIED_REGIONS**— Security Hub CSPM agrega datos de una lista seleccionada de regiones. Security Hub CSPM no agrega datos automáticamente de nuevas regiones. Se utiliza **Regions** para proporcionar la lista de regiones desde las que agregar.
- **NO_REGIONS**— Security Hub CSPM no agrega datos porque no seleccionas ninguna región vinculada.

En el siguiente ejemplo, se configura la agregación entre regiones. La región de origen es este de EE. UU. (norte de Virginia). Las regiones vinculadas son Oeste de EE. UU. (Norte de California) y Oeste de EE. UU. (Oregón). Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub create-finding-aggregator --region us-east-1 --region-linking-mode SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Revisión de la configuración de agregación entre regiones

Note

La región de agregación ahora se denomina región de origen. Algunas operaciones de la API CSPM de Security Hub siguen utilizando el antiguo término Región de agregación.

Puede ver la configuración actual de agregación entre regiones en AWS Security Hub Cloud Security Posture Management (CSPM) desde cualquier ubicación. Región de AWS La configuración incluye la región de origen, las regiones vinculadas (si las hay) y si se deben vincular automáticamente las nuevas regiones según lo admita Security Hub CSPM.

Las cuentas de miembro pueden ver la configuración de agregación entre regiones que configuró la cuenta de administrador.

Elija su método preferido y siga estos pasos para ver su configuración actual de agregación entre regiones.

Security Hub CSPM console

Para ver la configuración de agregación entre regiones (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Configuración y, luego, la pestaña Regiones.

Si la agregación entre regiones no está habilitada, la pestaña Regiones muestra la opción para habilitar la agregación entre regiones. Solo las cuentas de administrador y las cuentas independientes pueden habilitar la agregación entre regiones.

Si la agregación entre regiones está habilitada, la pestaña Regiones muestra la siguiente información:

- La región de origen
- Ya sea para agregar automáticamente los hallazgos, los conocimientos, los estados de control y las puntuaciones de seguridad de las nuevas regiones compatibles con Security Hub CSPM y por las que usted opte
- La lista de regiones vinculadas (si se selecciona alguna)

Security Hub CSPM API

Para revisar la configuración de agregación entre regiones (API CSPM de Security Hub)

Utilice el [GetFindingAggregator](#) funcionamiento de la API CSPM de Security Hub. Si usa el AWS CLI, ejecute el [get-finding-aggregator](#) comando.

Al realizar la solicitud, proporcione el ARN del agregador de resultados. Para obtener el ARN del agregador de resultados, utilice la operación [ListFindingAggregators](#) o el comando [list-finding-aggregators](#).

El siguiente ejemplo muestra la configuración de agregación entre regiones para el ARN del agregador de resultados especificado. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad

```
$aws securityhub get-finding-aggregator --finding-aggregator-  
arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-  
e89b-12d3-a456-426652340000
```

Actualización de la configuración de agregación entre regiones

Note

La región de agregación ahora se denomina región de origen. Algunas operaciones de la API CSPM de Security Hub siguen utilizando el antiguo término Región de agregación.

Puede actualizar su configuración actual de agregación entre regiones en AWS Security Hub Cloud Security Posture Management (CSPM) cambiando las regiones vinculadas o la región de origen actual. También puede cambiar si desea agregar automáticamente los datos de los nuevos Regiones de AWS que sean compatibles con el CSPM de Security Hub.

Los cambios en la agregación entre regiones no se implementan en una región opcional hasta que habilite la región en su Cuenta de AWS. Las regiones que AWS se introdujeron el 20 de marzo de 2019 o con posterioridad son regiones con suscripción voluntaria.

Cuando dejas de agregar datos de una región vinculada, AWS Security Hub Cloud Security Posture Management (CSPM) no elimina ningún dato agregado existente de esa región al que se pueda acceder en la región de origen.

No puede usar los procedimientos de actualización de esta sección para cambiar la región de origen. Para cambiar la región de origen, se debe hacer lo siguiente:

1. Detenga la agregación entre regiones. Para obtener instrucciones, consulte [the section called “Detención de la agregación”](#).
2. Cambie a la región que desea que sea la nueva región de origen.
3. Habilitación de agregación entre regiones. Para obtener instrucciones, consulte [the section called “Habilitación de agregación”](#).

Debe actualizar la configuración de agregación entre regiones desde la región de origen actual.

Security Hub CSPM console

Para cambiar las regiones vinculadas

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>

Inicie sesión en la región de agregación actual.

2. En el menú de navegación CSPM de Security Hub, seleccione Configuración y, a continuación, Regiones.
3. Para la opción Agregación de resultados, seleccione Editar.
4. Para la opción Regiones vinculadas, actualice las regiones vinculadas seleccionadas.
5. Si es necesario, cambie la selección de Vincular regiones futuras. Esta configuración determina si Security Hub CSPM vincula automáticamente las nuevas regiones a medida que añade soporte para ellas y usted opta por ellas.
6. Seleccione Save.

Security Hub CSPM API

Utilice la operación [UpdateFindingAggregator](#). Si usa el AWS CLI, ejecute el [update-finding-aggregator](#) comando. Para identificar el agregador de resultados, debe proporcionar el ARN de este. Para obtener el ARN del agregador de búsquedas, utilice [ListFindingAggregators](#) la operación o el comando.. [list-finding-aggregators](#)

Si el modo de enlace es ALL_REGIONS_EXCEPT_SPECIFIED o SPECIFIED_REGIONS, puede cambiar la lista de regiones excluidas o incluidas. Si quiere cambiar el modo de enlace de regiones a NO_REGIONS, no debe proporcionar una lista de regiones.

Al cambiar la lista de regiones excluidas o incluidas, debe proporcionar la lista completa con las actualizaciones. Por ejemplo, supongamos que actualmente agrega los resultados de Este de EE. UU. (Ohio) y desea agregar también los resultados de Oeste de EE. UU. (Oregón). Debe proporcionar una lista de Regions que contenga tanto el este de EE. UU. (Ohio) como el oeste de EE. UU. (Oregón).

En el siguiente ejemplo, se actualiza la agregación entre regiones para las regiones seleccionadas. El comando se ejecuta desde la región de origen actual, que es este de EE. UU. (norte de Virginia). Las regiones vinculadas son Oeste de EE. UU. (Norte de California) y Oeste de EE. UU. (Oregón). Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
aws securityhub update-finding-aggregator --region us-east-1 --finding-  
aggregator-arn arn:aws:securityhub:us-east-1:222222222222:finding-  
aggregator/123e4567-e89b-12d3-a456-426652340000 --region-linking-mode  
SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Detención de la agregación entre regiones

Note

La región de agregación ahora se denomina región de origen. Algunas operaciones de la API CSPM de Security Hub siguen utilizando el antiguo término Región de agregación.

Si no quieres que AWS Security Hub Cloud Security Posture Management (CSPM) agregue datos, puedes eliminar tu agregador de búsquedas. Como alternativa, puedes conservar tu agregador de búsquedas pero no vincular ninguna Región de AWS a la región de origen actualizando el agregador existente al modo de enlace. NO_REGIONS

Para cambiar su región de origen, debe eliminar su agregador de resultados actual y crear uno nuevo.

Al eliminar el agregador de búsquedas, Security Hub CSPM deja de agregar datos. No elimina ningún dato agregado existente de la región de origen.

Para eliminar el agregador de resultados (consola)

Puede eliminar su agregador de resultados únicamente desde la región de origen actual.

En regiones distintas de la región de origen, el panel Búsqueda de agregación de la consola CSPM de Security Hub muestra un mensaje en el que se indica que debe editar la configuración en la región de origen. Seleccione este mensaje para mostrar un enlace para cambiar a la región de origen.

Security Hub CSPM console

Para detener la agregación entre regiones (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. Asegúrese de que haya iniciado sesión en su región de origen actual.
3. En el menú de navegación CSPM de Security Hub, seleccione Configuración y, a continuación, Regiones.
4. En Agregación de resultados, seleccione Editar.

5. En Región de agregación, elija Sin región de agregación.
6. Seleccione Save.
7. En el cuadro de diálogo de confirmación, en el campo de confirmación, escriba **Confirm**.
8. Elija Confirmar.

Security Hub CSPM API

Utilice el [DeleteFindingAggregator](#) funcionamiento de la API CSPM de Security Hub. Si está utilizando el AWS CLI, ejecute el [delete-finding-aggregator](#) comando.

Para identificar el agregador de resultados que va a eliminar, proporcione el ARN de este. Para obtener el ARN del agregador de resultados, utilice la operación [ListFindingAggregators](#) o el comando [list-finding-aggregators](#).

En el siguiente ejemplo, se elimina el agregador de resultados. El comando se ejecuta desde la región de origen actual, que es este de EE. UU. (norte de Virginia). Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$aws securityhub delete-finding-aggregator arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000 --  
region us-east-1
```

Descripción de los estándares de seguridad en Security Hub (CSPM)

En AWS Security Hub Cloud Security Posture Management (CSPM), un estándar de seguridad es un conjunto de requisitos que se basa en los marcos normativos, las mejores prácticas del sector o las políticas de la empresa. Para obtener más información sobre los estándares que Security Hub CSPM admite actualmente, incluidos los controles de seguridad que se aplican a cada uno de ellos, consulte la [Referencia de estándares para Security Hub CSPM](#).

Al habilitar un estándar, Security Hub CSPM habilita automáticamente todos los controles que se aplican al estándar. A continuación, el Security Hub CSPM ejecuta comprobaciones de seguridad en los controles, lo que genera las conclusiones del Security Hub CSPM. Puede deshabilitar y volver a habilitar los controles individuales más adelante, según sea necesario. También puede desactivar un estándar por completo. Si deshabilita un estándar, Security Hub CSPM deja de ejecutar las comprobaciones de seguridad en los controles que se aplican al estándar. Ya no se generan resultados para los controles.

Además de los resultados, Security Hub CSPM genera una puntuación de seguridad para cada estándar que habilite. La puntuación se basa en el estado de los controles que se aplican al estándar. Si establece una región de agregación, la puntuación de seguridad de un estándar refleja el estado de los controles en todas las regiones vinculadas. Si es el administrador del Security Hub CSPM de una organización, la puntuación refleja el estado de los controles de todas las cuentas de la organización. Para obtener más información, consulte [Calcular las puntuaciones de seguridad](#).

Para revisar y gestionar los estándares, puede utilizar la consola CSPM de Security Hub o la API CSPM de Security Hub. En la consola, la página de estándares de seguridad muestra todos los estándares de seguridad que Security Hub CSPM admite actualmente. Incluye una descripción de cada estándar y su estado actual. Si habilita un estándar, también puede usar esta página para acceder a detalles adicionales del estándar. Por ejemplo, puedes revisar:

- La puntuación de seguridad actual del estándar.
- Estadísticas agregadas de los controles que se aplican al estándar.
- Una lista de los controles que se aplican a la norma y que están habilitados actualmente, incluido el estado de conformidad de cada uno de ellos.
- Una lista de los controles que se aplican a la norma pero que actualmente están deshabilitados.

Para un análisis más profundo, puede filtrar y ordenar los datos y profundizar para revisar los detalles de los controles individuales que se aplican a la norma.

Puede activar los estándares de forma individual para una sola cuenta y Región de AWS. Sin embargo, para ahorrar tiempo y reducir los errores de configuración en entornos con varias cuentas y regiones, le recomendamos que utilice una [configuración central](#) para habilitar y administrar los estándares. Con la configuración central, el administrador de CSPM de Security Hub delegado puede crear políticas que especifiquen cómo configurar un estándar en varias cuentas y regiones.

Temas

- [Referencia de estándares para Security Hub CSPM](#)
- [Habilitación de un estándar de seguridad](#)
- [Revisar los detalles de un estándar de seguridad](#)
- [Desactivar los estándares de seguridad activados automáticamente](#)
- [Deshabilitación de un estándar de seguridad](#)

Referencia de estándares para Security Hub CSPM

En AWS Security Hub Cloud Security Posture Management (CSPM), un estándar de seguridad es un conjunto de requisitos que se basa en los marcos normativos, las mejores prácticas del sector o las políticas de la empresa. Security Hub CSPM asigna estos requisitos a los controles y ejecuta comprobaciones de seguridad en los controles para evaluar si se cumplen los requisitos de un estándar. Cada estándar incluye varios controles.

Security Hub CSPM admite actualmente los siguientes estándares:

- **AWS Mejores prácticas fundamentales de seguridad:** desarrollado por profesionales del sector AWS y desarrollado por profesionales del sector, es una recopilación de las mejores prácticas de seguridad para organizaciones, independientemente de su sector o tamaño. Proporciona un conjunto de controles que detectan cuándo usted Cuentas de AWS y sus recursos se desvían de las mejores prácticas de seguridad. También proporciona orientación prescriptiva sobre cómo mejorar y mantener su postura de seguridad.
- **AWS Etiquetado de recursos:** desarrollado por Security Hub CSPM, este estándar puede ayudarlo a determinar si sus AWS recursos tienen etiquetas. Una etiqueta es un par clave-valor que actúa como metadatos de un recurso. AWS Las etiquetas pueden ayudarlo a identificar, categorizar, administrar y buscar recursos. AWS Por ejemplo, puede usar etiquetas para clasificar los recursos por propósito, propietario o entorno.

- CIS AWS Foundations Benchmark: desarrollado por el Centro de Seguridad de Internet (CIS), este estándar proporciona pautas de configuración segura para AWS. Especifica un conjunto de pautas de configuración de seguridad y mejores prácticas para un subconjunto de recursos Servicios de AWS y hace hincapié en las configuraciones fundamentales, comprobables y independientes de la arquitectura. Las directrices incluyen procedimientos claros de step-by-step implementación y evaluación.
- Revisión 5 del NIST SP 800-53: esta norma se ajusta a los requisitos del Instituto Nacional de Estándares y Tecnología (NIST) para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información y los recursos críticos. El marco asociado generalmente se aplica a las agencias u organizaciones federales de EE. UU. que trabajan con las agencias federales o los sistemas de información de los EE. UU. Sin embargo, las organizaciones privadas también pueden utilizar los requisitos como marco orientativo.
- Revisión 2 del NIST SP 800-171: esta norma se ajusta a las recomendaciones y requisitos de seguridad del NIST para proteger la confidencialidad de la información no clasificada controlada (CUI) en sistemas y organizaciones que no forman parte del gobierno federal de los EE. UU. La CUI es información que no cumple con los criterios gubernamentales de clasificación, pero que se considera confidencial y que ha sido creada o poseída por el gobierno federal de los EE. UU. u otras entidades en nombre del gobierno federal de los EE. UU.
- PCI DSS: esta norma se ajusta al marco de conformidad con el estándar de seguridad de datos del sector de las tarjetas de pago (PCI DSS) definido por el Consejo de Normas de Seguridad de la PCI (SSC). El marco proporciona un conjunto de normas y directrices para gestionar de forma segura la información de las tarjetas de crédito y débito. El marco generalmente se aplica a las organizaciones que almacenan, procesan o transmiten datos de titulares de tarjetas.
- Estándar gestionado por servicios AWS Control Tower: este estándar le ayuda a configurar los controles proactivos proporcionados AWS Control Tower junto con los controles de detección proporcionados por Security Hub CSPM. AWS Control Tower ofrece una forma sencilla de configurar y gobernar un entorno de AWS múltiples cuentas, siguiendo las mejores prácticas prescriptivas. Al habilitar controles proactivos y de detección para su AWS entorno, puede mejorar su postura de seguridad en las diferentes etapas de desarrollo.

Los estándares y controles del CSPM de Security Hub no garantizan el cumplimiento de ningún marco regulatorio o auditoría. Por el contrario, proporcionan una forma de evaluar y monitorear el estado de sus recursos Cuentas de AWS . Te recomendamos que habilite cada estándar que sea relevante para las necesidades, el sector o el caso de uso de tu empresa.

Los controles individuales se pueden aplicar a más de un estándar. Si habilita varios estándares, le recomendamos que también habilite los hallazgos de control consolidados. Si lo hace, Security Hub CSPM genera un único resultado para cada control, incluso si el control se aplica a más de un estándar. Si no activa las conclusiones de control consolidadas, Security Hub CSPM genera una conclusión independiente para cada estándar habilitado al que se aplique un control. Por ejemplo, si habilita dos estándares y se aplica un control a ambos, recibirá dos resultados distintos para el control, uno para cada estándar. Si habilita las conclusiones de control consolidadas, recibirá solo una conclusión para el control. Para obtener más información, consulte [Resultados de control consolidados](#).

Referencia detallada por norma

- [AWS Estándar fundamental de mejores prácticas de seguridad en Security Hub \(CSPM\)](#)
- [AWS Estándar de etiquetado de recursos en Security Hub \(CSPM\)](#)
- [CIS AWS Foundations es el punto de referencia en Security Hub \(CSPM\)](#)
- [NIST SP 800-53 revisión 5 en Security Hub CSPM](#)
- [NIST SP 800-171 revisión 2 en Security Hub CSPM](#)
- [PCI DSS en Security Hub CSPM](#)
- [Estándares gestionados por servicios en Security Hub CSPM](#)

AWS Estándar fundamental de mejores prácticas de seguridad en Security Hub (CSPM)

Desarrollado por profesionales de la industria AWS y desarrollado por profesionales del sector, el estándar de mejores prácticas de seguridad AWS fundamentales (FSBP) es una recopilación de las mejores prácticas de seguridad para organizaciones, independientemente del sector o tamaño de la organización. Proporciona un conjunto de controles que detectan cuándo Cuentas de AWS y los recursos se desvían de las mejores prácticas de seguridad. También proporciona orientación prescriptiva sobre cómo mejorar y mantener la postura de seguridad de su organización.

En AWS Security Hub Cloud Security Posture Management (CSPM), el estándar AWS Foundational Security Best Practices incluye controles que evalúan continuamente sus cargas de trabajo y las de usted, Cuentas de AWS y le ayudan a identificar las áreas que se desvían de las mejores prácticas de seguridad. Los controles incluyen las mejores prácticas de seguridad para los recursos de varios Servicios de AWS. A cada control se le asigna una categoría que refleja la función de

seguridad a la que se aplica el control. Para obtener una lista de categorías y detalles adicionales, consulte [Categorías de control](#).

Controles que se aplican a la norma

La siguiente lista especifica qué controles de AWS Security Hub Cloud Security Posture Management (CSPM) se aplican al estándar AWS Foundational Security Best Practices (v1.0.0). Para revisar los detalles de un control, selecciónelo.

[\[Cuenta.1\] La información de contacto de seguridad debe proporcionarse para un Cuenta de AWS](#)

[\[ACM.1\] Los certificados importados y emitidos por ACM deben renovarse después de un período de tiempo específico](#)

[\[ACM.2\] Los certificados RSA administrados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)

[\[APIGateway.1\] El registro de ejecución de WebSocket REST y API de API Gateway debe estar habilitado](#)

[\[APIGateway.2\] Las etapas de la API de REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend](#)

[\[APIGateway.3\] Las etapas de la API de REST de API Gateway tener AWS X-Ray habilitado el rastreo](#)

[\[APIGateway.4\] La API Gateway debe estar asociada a una ACL web de WAF](#)

[\[APIGateway.5\] Los datos de la caché de la API de REST de API Gateway deben cifrarse en reposo](#)

[\[APIGateway.8\] Las rutas de API Gateway deben especificar un tipo de autorización](#)

[\[APIGateway.9\] El registro de acceso debe configurarse para las etapas V2 de API Gateway](#)

[\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)

[\[AppSync.2\] AWS AppSync debe tener habilitado el registro a nivel de campo](#)

[\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves de API](#)

[\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)

[\[Athena.4\] Los grupos de trabajo de Athena deben tener el registro habilitado](#)

[\[AutoScaling.1\] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar las comprobaciones de estado del ELB](#)

[\[AutoScaling.2\] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad](#)

[\[AutoScaling.3\] Las configuraciones de lanzamiento de grupos de Auto Scaling deberían configurar las EC2 instancias para que requieran la versión 2 del Servicio de Metadatos de Instancia \(IMDSv2\)](#)

[\[AutoScaling.5\] EC2 Las instancias de Amazon lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas](#)

[\[AutoScaling.6\] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad](#)

[\[AutoScaling.9\] Los grupos de Amazon EC2 Auto Scaling deberían usar las plantillas de EC2 lanzamiento de Amazon](#)

[\[Backup.1\] Los puntos AWS Backup de recuperación deben cifrarse en reposo](#)

[\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)

[\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)

[\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)

[\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)

[\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)

[\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)

[\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)

[\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)

[\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)

[\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)

[\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)

[\[CloudTrail.1\] CloudTrail debe habilitarse y configurarse con al menos un registro de seguimiento para varias regiones que incluya eventos de administración de lectura y escritura](#)

[\[CloudTrail.2\] CloudTrail debe tener habilitado el cifrado en reposo](#)

[\[CloudTrail.4\] La validación de archivo de CloudTrail registro debe estar habilitada](#)

[\[CloudTrail.5\] CloudTrail Los senderos deben estar integrados con Amazon Logs CloudWatch](#)

[\[CodeBuild.1\] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales](#)

[\[CodeBuild.2\] Las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro](#)

[\[CodeBuild.3\] Los registros de CodeBuild S3 deben estar cifrados](#)

[\[CodeBuild.4\] Los entornos de los CodeBuild proyectos deben tener una duración de registro AWS Config](#)

[\[CodeBuild.7\] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo](#)

[\[Config.1\] AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos](#)

[\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)

[\[DataFirehose.1\] Los flujos de entrega de Firehose deben cifrarse en reposo](#)

[\[DataSync.1\] DataSync las tareas deberían tener el registro activado](#)

[\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)

[\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias](#)

[\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)

[\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)

[\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)

[\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)

[\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado](#)

[\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado](#)

[\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)

[\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)

[\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)

[\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)

[\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)

[\[DocumentDb.6\] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito](#)

[\[DynamoDB.1\] Las tablas de DynamoDB deberían escalar automáticamente la capacidad en función de la demanda](#)

[\[DynamoDB.2\] Las tablas de DynamoDB deben tener habilitada la recuperación point-in-time](#)

[\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)

[\[DynamoDB.6\] Las tablas de DynamoDB deben tener la protección contra eliminación habilitada](#)

[\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)

[\[EC2.1\] Las instantáneas de Amazon EBS no se deben poder restaurar públicamente](#)

[\[EC22\] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente](#)

[\[EC2.3\] Los volúmenes de Amazon EBS asociados deben cifrarse en reposo](#)

[\[EC24\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)

[\[EC2.6\] El registro de flujos de VPC debe estar habilitado en todos VPCs](#)

[\[EC2.7\] El cifrado predeterminado de EBS debe estar activado](#)

[\[EC2.8\] EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancias IMDSv2](#)

[\[EC2.9\] EC2 Las instancias de Amazon no deben tener una dirección pública IPv4](#)

[\[EC2.10\] Amazon EC2 debe configurarse para utilizar los puntos de enlace de VPC que se crean para el servicio de Amazon EC2](#)

[\[EC215\] EC2 Las subredes de Amazon no deben asignar automáticamente direcciones IP públicas](#)

[\[EC2.16\] Deben eliminarse las listas de control de acceso a la red no utilizadas](#)

[\[EC2.17\] EC2 Las instancias de Amazon no deberían usar múltiples ENIs](#)

[\[EC2.18\] Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados](#)

[\[EC219\] Los grupos de seguridad no deben permitir el acceso irrestricto a los puertos de alto riesgo](#)

[\[EC220\] Ambos túneles de VPN de una conexión de AWS Site-to-Site VPN deben estar activos](#)

[\[EC2.21\] La red no ACLs debe permitir la entrada desde 0.0.0/0 al puerto 22 o al puerto 3389](#)

[\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)

[\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)

[\[EC2.25\] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red](#)

[\[EC251\] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)

[\[EC2.55\] VPCs debe configurarse con un punto final de interfaz para la API ECR](#)

[\[EC2.56\] VPCs debe configurarse con un punto final de interfaz para Docker Registry](#)

[\[EC2.57\] VPCs debe configurarse con un punto final de interfaz para Systems Manager](#)

[\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)

[\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)

[\[EC2.170\] Las plantillas de EC2 lanzamiento deben usar el servicio de metadatos de instancias versión 2 \(\) IMDSv2](#)

[\[EC2.171\] Las conexiones EC2 VPN deben tener el registro habilitado](#)

[\[EC2.172\] La configuración del acceso público al bloqueo de EC2 VPC debería bloquear el tráfico de las puertas de enlace de Internet](#)

[\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)

[\[ECR.1\] Los repositorios privados del ECR deben tener configurado el escaneo de imágenes](#)

[\[ECR.2\] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas](#)

[\[ECR.3\] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida](#)

[\[ECS.1\] Las definiciones de tareas de Amazon ECS deben tener modos de red seguros y definiciones de usuario](#)

[\[ECS.2\] Los servicios de ECS no deberían tener direcciones IP públicas asignadas automáticamente](#)

[\[ECS.3\] Las definiciones de tareas de ECS no deben compartir el espacio de nombres de los procesos del anfitrión](#)

[\[ECS.4\] Los contenedores de ECS deben ejecutarse sin privilegios](#)

[\[ECS.5\] Los contenedores ECS deben limitarse al acceso de solo lectura a los sistemas de archivos raíz](#)

[\[ECS.8\] Los secretos no deben pasarse como variables de entorno del contenedor](#)

[\[ECS.9\] Las definiciones de tareas de ECS deben tener una configuración de registro](#)

[\[ECS.10\] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate](#)

[\[ECS.12\] Los clústeres de ECS deben usar Container Insights](#)

[\[ECS.16\] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas](#)

[\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)

[\[EFS.2\] Los volúmenes de Amazon EFS deben estar en los planes de respaldo](#)

[\[EFS.3\] Los puntos de acceso EFS deben aplicar un directorio raíz](#)

[\[EFS.4\] Los puntos de acceso EFS deben imponer una identidad de usuario](#)

[\[EFS.6\] Los destinos de montaje de EFS no deben estar asociados a una subred pública](#)

[\[EFS.7\] Los sistemas de archivos de EFS deben tener habilitadas las copias de seguridad automáticas](#)

[\[EFS.8\] Los sistemas de archivos de EFS deben cifrarse en reposo](#)

[\[EKS.1\] Los puntos de enlace del clúster EKS no deben ser de acceso público](#)

[\[EKS.2\] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible](#)

[\[EKS.3\] Los clústeres de EKS deben usar secretos de Kubernetes cifrados](#)

[\[EKS.8\] Los clústeres de EKS deben tener habilitado el registro de auditoría](#)

[\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)

[\[ElastiCache.2\] ElastiCache Los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias](#)

[\[ElastiCache.3\] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática](#)

[\[ElastiCache.4\] los grupos de ElastiCache replicación deben estar cifrados en reposo](#)

[\[ElastiCache.5\] los grupos de ElastiCache replicación deben cifrarse en tránsito](#)

[\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)

[\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)

[\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)

[\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)

[\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)

[\[ELB.1\] El equilibrador de carga de aplicación debe configurarse para redirigir todas las solicitudes HTTP a HTTPS](#)

[\[ELB.2\] Los equilibradores de carga clásicos con agentes de escucha SSL/HTTPS deben usar un certificado proporcionado por AWS Certificate Manager](#)

[\[ELB.3\] Los oyentes de Equilibrador de carga clásico deben configurarse con una terminación HTTPS o TLS](#)

[\[ELB.4\] El equilibrador de carga de aplicación debe configurarse para eliminar los encabezados http no válidos](#)

[\[ELB.5\] El registro de las aplicaciones y de los equilibradores de carga clásicos debe estar habilitado](#)

[\[ELB.6\] La protección contra la eliminación de un equilibrador de carga de aplicación, de puerta de enlace y de red debe estar habilitada](#)

[\[ELB.7\] Los equilibradores de carga clásicos deberían tener habilitado el drenaje de conexiones](#)

[\[ELB.8\] Los equilibradores de carga clásicos con agentes de escucha SSL deben usar una política de seguridad predefinida que tenga una duración sólida AWS Config](#)

[\[ELB.9\] Los equilibradores de carga clásicos deberían tener habilitado el equilibrio de carga entre zonas](#)

[\[ELB.10\] Equilibrador de carga clásico debe abarcar varias zonas de disponibilidad](#)

[\[ELB.12\] Equilibrador de carga de aplicación debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)

[\[ELB.13\] Los equilibradores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad](#)

[\[ELB.14\] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)

[\[ELB.17\] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas](#)

[\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)

[\[EMR.2\] La configuración de bloqueo del acceso público de Amazon EMR debe estar habilitada](#)

[\[EMR.3\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo](#)

[\[EMR.4\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito](#)

[\[ES.1\] Los dominios de Elasticsearch deben tener habilitado el cifrado en reposo](#)

[\[ES.2\] Los dominios de Elasticsearch no deben ser de acceso público](#)

[\[ES.3\] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos](#)

[\[ES.4\] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros](#)

[\[ES.5\] Los dominios de Elasticsearch deben tener habilitado el registro de auditoría](#)

[\[ES.6\] Los dominios de Elasticsearch deben tener al menos tres nodos de datos](#)

[\[ES.7\] Los dominios de Elasticsearch deben configurarse con al menos tres nodos maestros dedicados](#)

[\[ES.8\] Las conexiones a dominios de Elasticsearch deben estar cifradas conforme a la política de seguridad TLS más reciente](#)

[\[EventBridge.3\] Los autobuses de eventos EventBridge personalizados deben incluir una política basada en los recursos](#)

[\[FSx.1\] en el caso FSx de OpenZFS, los sistemas de archivos deben configurarse para copiar etiquetas en copias de seguridad y volúmenes](#)

[\[FSx.2\] FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad](#)

[\[FSx.3\] FSx para los sistemas de archivos OpenZFS, debe configurarse para el despliegue en zonas de disponibilidad múltiples](#)

[\[FSx.4\] FSx para los sistemas de archivos NetApp ONTAP, debe configurarse para el despliegue en zonas de disponibilidad múltiples](#)

[\[FSx.5\] FSx para Windows, los sistemas de archivos del servidor de archivos deben configurarse para el despliegue en zonas de disponibilidad múltiples](#)

[\[Glue.3\] Las transformaciones AWS Glue de aprendizaje automático deben cifrarse en reposo](#)

[\[Glue.4\] Los trabajos de AWS Glue Spark deberían ejecutarse en versiones compatibles de AWS Glue](#)

[\[GuardDuty.1\] GuardDuty debería estar activado](#)

[\[GuardDuty.5\] La supervisión de registros de auditoría de GuardDuty EKS debe estar habilitada](#)

[\[GuardDuty.6\] La protección de GuardDuty Lambda debe estar habilitada](#)

[\[GuardDuty.7\] La supervisión en tiempo de ejecución de GuardDuty EKS debe estar habilitada](#)

[\[GuardDuty.8\] La protección contra GuardDuty malware para EC2 debe estar habilitada](#)

[\[GuardDuty.9\] La protección de GuardDuty RDS debe estar habilitada](#)

[\[GuardDuty.10\] La protección de GuardDuty S3 debe estar habilitada](#)

[\[GuardDuty.11\] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada](#)

[\[GuardDuty.12\] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada](#)

[\[GuardDuty.13\] La monitorización del GuardDuty EC2 tiempo de ejecución debe estar habilitada](#)

[\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)

[\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)

[\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)

[\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)

[\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)

[\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)

[\[IAM.7\] Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras](#)

[\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)

[\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)

[\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)

[\[Inspector.2\] El análisis de ECR en Amazon Inspector debe estar habilitado](#)

[\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)

[\[Inspector.4\] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado](#)

[\[Kinesis.1\] Las transmisiones de Kinesis deben cifrarse en reposo](#)

[\[Kinesis.3\] Las transmisiones de Kinesis deben tener un periodo adecuado de retención de datos](#)

[\[KMS.1\] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS](#)

[\[KMS.2\] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS](#)

[\[KMS.3\] no AWS KMS keys debe eliminarse involuntariamente](#)

[\[KMS.5\] Las claves KMS no deben ser de acceso público](#)

[\[Lambda.1\] Las políticas de función de Lambda deberían prohibir el acceso público](#)

[\[Lambda.2\] Las funciones de Lambda deben usar los tiempos de ejecución admitidos](#)

[\[Lambda.5\] Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad](#)

[\[Macie.1\] Amazon Macie debe estar habilitado](#)

[\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)

[\[MQ.2\] Los corredores de ActiveMQ deberían transmitir los registros de auditoría a CloudWatch](#)

[\[MQ.3\] Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias](#)

[\[MSK.1\] Los clústeres de MSK deben cifrarse en tránsito entre los nodos intermediarios](#)

[\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)

[\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo](#)

[\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)

[\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)

[\[Neptune.4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación](#)

[\[Neptune.5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas](#)

[\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)

[\[Neptune.7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM](#)

[\[Neptune.8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas](#)

[\[NetworkFirewall.2\] El registro de Network Firewall debe estar habilitado](#)

[\[NetworkFirewall.3\] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas](#)

[\[NetworkFirewall.4\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos](#)

[\[NetworkFirewall.5\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados](#)

[El grupo de reglas de Stateless Network Firewall \[NetworkFirewall.6\] no debe estar vacío](#)

[Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de eliminación](#)

[Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de cambio de subred](#)

Los OpenSearch dominios [Opensearch.1] deben tener activado el cifrado en reposo

Los OpenSearch dominios [Opensearch.2] no deben ser de acceso público

Los OpenSearch dominios [Opensearch.3] deben cifrar los datos enviados entre nodos

El registro de errores de OpenSearch dominio [Opensearch.4] en CloudWatch Logs debe estar activado

Los OpenSearch dominios [Opensearch.5] deben tener habilitado el registro de auditoría

Los OpenSearch dominios [Opensearch.6] deben tener al menos tres nodos de datos

Los OpenSearch dominios [Opensearch.7] deben tener habilitado un control de acceso detallado

[Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente

Los OpenSearch dominios [Opensearch.10] deben tener instalada la última actualización de software

La autoridad emisora de certificados AWS Private CA raíz [PCA.1] debe estar deshabilitada

Las zonas alojadas públicas de Route 53 [Route53.2] deben registrar las consultas de DNS

[RDS.1] La instantánea de RDS debe ser privada

[RDS.2] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible

[RDS.3] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo

Las instantáneas de clústeres y bases de datos de RDS [RDS.4] deben cifrarse cuando están inactivas

Las instancias de base de datos de RDS [RDS.5] deben configurarse con varias zonas de disponibilidad

Se debe configurar una supervisión mejorada para las instancias de base de datos de RDS [RDS.6]

Los clústeres de RDS [RDS.7] deben tener habilitada la protección contra la eliminación

Las instancias de base de datos de RDS [RDS.8] deben tener habilitada la protección contra la eliminación

[\[RDS.9\] Las instancias de base de datos de RDS deben publicar los registros en Logs CloudWatch](#)

[La autenticación de IAM \[RDS.10\] debe configurarse para las instancias de RDS](#)

[Las instancias RDS \[RDS.11\] deben tener habilitadas las copias de seguridad automáticas](#)

[La autenticación de IAM \[RDS.12\] debe configurarse para los clústeres de RDS](#)

[Las actualizaciones automáticas de las versiones secundarias de RDS \[RDS.13\] deben estar habilitadas](#)

[Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)

[Los clústeres de bases de datos de RDS \[RDS.15\] deben configurarse para varias zonas de disponibilidad](#)

[Los clústeres de bases de datos de RDS \[RDS.16\] deben configurarse para copiar etiquetas en las instantáneas](#)

[Las instancias de base de datos de RDS \[RDS.17\] deben configurarse para copiar etiquetas en las instantáneas](#)

[Las suscripciones de notificación de eventos de RDS \[RDS.19\] existentes deben configurarse para los eventos de clúster críticos](#)

[Las suscripciones de notificación de eventos de RDS \[RDS.20\] existentes deben configurarse para eventos críticos de instancias de bases de datos](#)

[Se debe configurar una suscripción a las notificaciones de eventos de RDS \[RDS.21\] para los eventos críticos de los grupos de parámetros de bases de datos](#)

[Se debe configurar una suscripción a las notificaciones de eventos de RDS \[RDS.22\] para los eventos críticos de los grupos de seguridad de bases de datos](#)

[Las instancias RDS \[RDS.23\] no deben usar el puerto predeterminado de un motor de base de datos](#)

[Los clústeres de bases de datos de RDS \[RDS.24\] deben usar un nombre de usuario de administrador personalizado](#)

[Las instancias de bases de datos de RDS \[RDS.25\] deben usar un nombre de usuario de administrador personalizado](#)

[Los clústeres de bases de datos de RDS \[RDS.27\] deben cifrarse en reposo](#)

[\[RDS.34\] Los clústeres de bases de datos Aurora MySQL deberían publicar los registros de auditoría en Logs CloudWatch](#)

[Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)

[\[RDS.36\] Las instancias de base de datos de RDS para PostgreSQL deben publicar registros en Logs CloudWatch](#)

[\[RDS.37\] Los clústeres de bases de datos Aurora PostgreSQL deberían publicar registros en Logs CloudWatch](#)

[\[RDS.40\] Las instancias de base de datos de RDS para SQL Server deberían publicar los registros en Logs CloudWatch](#)

[\[RDS.41\] Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito](#)

[\[RDS.42\] Las instancias de base de datos de RDS para MariaDB deberían publicar registros en Logs CloudWatch](#)

[\[RDS.44\] El RDS para las instancias de base de datos MariaDB debe cifrarse en tránsito](#)

[\[Redshift.1\] Los clústeres de Amazon Redshift deberían prohibir el acceso público](#)

[Las conexiones a los clústeres de Amazon Redshift \[Redshift.2\] deben cifrarse en tránsito](#)

[Los clústeres de Amazon Redshift \[Redshift.3\] deben tener habilitadas las instantáneas automáticas](#)

[Los clústeres de Amazon Redshift \[Redshift.4\] deben tener habilitado el registro de auditoría](#)

[Amazon Redshift \[Redshift.6\] debería tener habilitadas las actualizaciones automáticas a las versiones principales](#)

[Los clústeres de Redshift \[Redshift.7\] deberían utilizar un enrutamiento de VPC mejorado](#)

[Los clústeres de Amazon Redshift \[Redshift.8\] no deben usar el nombre de usuario de administrador predeterminado](#)

[Los clústeres de Redshift \[Redshift.9\] no deben usar el nombre de base de datos predeterminado](#)

[Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo](#)

[\[Redshift.15\] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos](#)

[Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)

[\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)

[\[RedshiftServerless.3\] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público](#)

[Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado](#)

[\[RedshiftServerless.6\] Los espacios de nombres de Redshift Serverless deberían exportar los registros a los registros CloudWatch](#)

[Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de base de datos predeterminado](#)

[\[S3.1\] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público](#)

[\[S3.2\] Los buckets de uso general de S3 deben bloquear el acceso público de lectura](#)

[\[S3.3\] Los buckets de uso general de S3 deben bloquear el acceso público de escritura](#)

[\[S3.5\] En las solicitudes de los buckets de uso general de S3, se debe pedir el uso de SSL](#)

[\[S3.6\] Las políticas de compartimentos de uso general de S3 deberían restringir el acceso a otras Cuentas de AWS](#)

[\[S3.8\] Los buckets de uso general de S3 deben bloquear el acceso público](#)

[\[S3.9\] Los buckets de uso general de S3 deben tener habilitado el registro de acceso al servidor](#)

[\[S3.12\] no ACLs debe usarse para administrar el acceso de los usuarios a los depósitos de uso general de S3](#)

[\[S3.13\] Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida](#)

[\[S3.19\] Los puntos de acceso de S3 deben tener habilitada la configuración de Bloqueo de acceso público](#)

[\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)

[\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)

[\[SageMaker.2\] las instancias de SageMaker notebook deben lanzarse en una VPC personalizada](#)

[\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook](#)

[\[SageMaker.4\] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1](#)

[\[SageMaker.5\] SageMaker los modelos deberían bloquear el tráfico entrante](#)

[\[SageMaker.8\] las instancias de SageMaker notebook deberían ejecutarse en plataformas compatibles](#)

[\[SecretsManager.1\] Los secretos de Secrets Manager deberían tener habilitada la rotación automática](#)

[\[SecretsManager.2\] Los secretos de Secrets Manager configurados con rotación automática deberían rotar correctamente](#)

[\[SecretsManager.3\] Eliminar los secretos de Secrets Manager no utilizados](#)

[\[SecretsManager.4\] Los secretos de Secrets Manager deben rotarse en un número específico de días](#)

[\[ServiceCatalog.1\] Las carteras de Service Catalog solo deben compartirse dentro de una AWS organización](#)

[\[SNS.4\] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público](#)

[Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)

[\[SQS.3\] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público](#)

[\[SSM.1\] EC2 Las instancias de Amazon deben administrarse mediante AWS Systems Manager](#)

[\[SSM.2\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de parche de COMPLIANT después de la instalación de un parche](#)

[\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)

[\[SSM.4\] Los documentos SSM no deben ser públicos](#)

[\[StepFunctions.1\] Las máquinas de estado de Step Functions deberían tener el registro activado](#)

[\[Transfer.2\] Los servidores de Transfer Family no deben utilizar el protocolo FTP para la conexión del punto de conexión](#)

[\[Transfer.3\] Los conectores Transfer Family deben tener habilitado el registro](#)

[El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)

[Las reglas de \[WAF.2\] Regionales AWS WAF clásicas deben tener al menos una condición](#)

[Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)

[La web de \[WAF.4\] Regionales AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

[Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)

[Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)

[La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

[La AWS WAF web de \[WAF.10\] ACLs debe tener al menos una regla o grupo de reglas](#)

[AWS WAF Las reglas de \[WAF.12\] deben tener habilitadas las métricas CloudWatch](#)

[\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)

[\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

AWS Estándar de etiquetado de recursos en Security Hub (CSPM)

El estándar de etiquetado de AWS recursos, desarrollado por AWS Security Hub Cloud Security Posture Management (CSPM), le ayuda a determinar si a sus AWS recursos les faltan etiquetas. Las etiquetas son pares clave-valor que actúan como metadatos para organizar los recursos. AWS En la mayoría de AWS los recursos, tiene la opción de añadir etiquetas a un recurso al crearlo o después de crearlo. Entre los ejemplos de recursos se incluyen CloudFront las distribuciones de Amazon, las

instancias de Amazon Elastic Compute Cloud (Amazon EC2) y los secretos de entrada. AWS Secrets Manager Las etiquetas pueden ayudarle a administrar, identificar, organizar, buscar y filtrar AWS los recursos.

Cada etiqueta de tiene dos partes:

- Una clave de etiqueta, por ejemplo, CostCenterEnvironment, o. Project Las claves de etiqueta distinguen entre mayúsculas y minúsculas.
- Un valor de etiqueta, por ejemplo, o. 111122223333 Production Al igual que las claves de etiqueta, los valores de etiqueta distinguen entre mayúsculas y minúsculas.

Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Para obtener información sobre cómo añadir etiquetas a AWS los recursos, consulte la Guía del usuario de [Tagging AWS Resources y Tag Editor](#).

Para cada control que se aplique al estándar de etiquetado de AWS recursos de Security Hub CSPM, puede utilizar opcionalmente el parámetro compatible para especificar las claves de etiqueta que desea que compruebe el control. Si no especifica ninguna clave de etiqueta, el control solo comprueba la existencia de al menos una clave de etiqueta y falla si un recurso no tiene ninguna clave de etiqueta.

Antes de activar el estándar de etiquetado de AWS recursos, es importante activar y configurar primero el registro de recursos en AWS Config. Al configurar el registro de recursos, asegúrese también de habilitarlo para todos los tipos de AWS recursos que se comprueban mediante los controles que se aplican al estándar. De lo contrario, es posible que Security Hub CSPM no pueda evaluar los recursos adecuados y generar resultados precisos para los controles que se aplican a la norma. Para obtener más información, incluida una lista de los tipos de recursos que se deben registrar, consulte. [AWS Config Recursos necesarios para los hallazgos de control](#)

 Note

El estándar AWS de etiquetado de recursos no está disponible en el oeste de Canadá (Calgary), China y las regiones. AWS GovCloud (US)

Tras activar el estándar de etiquetado de AWS recursos, empezará a recibir información sobre los controles que se aplican al estándar. Tenga en cuenta que Security Hub CSPM puede tardar hasta 18 horas en generar resultados para los controles que utilizan la misma regla AWS Config

vinculada a servicios que los controles que se aplican a otros estándares habilitados. Para obtener más información, consulte [Programación para ejecutar comprobaciones de seguridad](#).

El estándar AWS de etiquetado de recursos tiene el siguiente nombre de recurso de Amazon (ARN): `arn:aws:securityhub:region::standards/aws-resource-tagging-standard/v/1.0.0`. También puede utilizar el [GetEnabledStandards](#) funcionamiento de la API CSPM de Security Hub para encontrar el ARN de un estándar habilitado.

Controles que se aplican al estándar

En la siguiente lista se especifican los controles de AWS Security Hub Cloud Security Posture Management (CSPM) que se aplican al estándar de etiquetado de AWS recursos (v1.0.0). Para revisar los detalles de un control, selecciónelo.

- [\[ACM.3\] Los certificados ACM deben estar etiquetados](#)
- [\[Amplify.1\] Las aplicaciones de Amplify deben estar etiquetadas](#)
- [\[Amplify.2\] Las ramas de Amplify deben estar etiquetadas](#)
- [\[AppConfig.1\] AWS AppConfig las aplicaciones deben estar etiquetadas](#)
- [\[AppConfig.2\] los perfiles de AWS AppConfig configuración deben estar etiquetados](#)
- [\[AppConfig.3\] AWS AppConfig los entornos deben estar etiquetados](#)
- [\[AppConfig.4\] Las asociaciones AWS AppConfig de extensiones deben estar etiquetadas](#)
- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.4\] AWS AppSync APIs GraphQL debe estar etiquetado](#)
- [\[Athena.2\] Los catálogos de datos de Athena deben estar etiquetados](#)
- [\[Athena.3\] Los grupos de trabajo de Athena deben estar etiquetados](#)
- [\[AutoScaling.10\] Los grupos EC2 de Auto Scaling deben estar etiquetados](#)
- [\[Backup.2\] Los puntos AWS Backup de recuperación deben estar etiquetados](#)
- [\[Backup.3\] las AWS Backup bóvedas deben estar etiquetadas](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[Backup.5\] los planes de AWS Backup respaldo deben estar etiquetados](#)
- [\[Batch.1\] Las colas de trabajos por lotes deben estar etiquetadas](#)

- [\[Batch.2\] Las políticas de programación de lotes deben estar etiquetadas](#)
- [\[Batch.3\] Los entornos de procesamiento por lotes deben etiquetarse](#)
- [\[Batch.4\] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben etiquetarse](#)
- [\[CloudFormation.2\] las CloudFormation pilas deben estar etiquetadas](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CloudTrail.9\] los registros de CloudTrail seguimiento deben etiquetarse](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[DataSync.2\] DataSync las tareas deben estar etiquetadas](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.2\] Los certificados DMS deben estar etiquetados](#)
- [\[DMS.3\] Las suscripciones a eventos de DMS deben estar etiquetadas](#)
- [\[DMS.4\] Las instancias de replicación de DMS deben etiquetarse](#)
- [\[DMS.5\] Los grupos de subredes de replicación del DMS deben estar etiquetados](#)
- [\[DynamoDB.5\] Las tablas de DynamoDB deben etiquetarse](#)
- [\[EC2.33\] Las conexiones de puerta de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.34\] Las tablas de enrutamiento de las puertas de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.35\] Las interfaces EC2 de red deben etiquetarse](#)
- [\[EC2.36\] Las pasarelas de EC2 clientes deben estar etiquetadas](#)
- [\[EC2.37\] Las direcciones IP EC2 elásticas deben etiquetarse](#)
- [\[EC2.38\] EC2 las instancias deben estar etiquetadas](#)
- [\[EC2.39\] Las puertas de enlace de EC2 Internet deben etiquetarse](#)
- [\[EC2.40\] Las puertas de enlace de EC2 NAT deben etiquetarse](#)
- [La EC2 red \[EC2.41\] ACLs debe estar etiquetada](#)
- [\[EC2.42\] Las tablas de EC2 enrutamiento deben estar etiquetadas](#)

- [\[EC2.43\] los grupos EC2 de seguridad deben estar etiquetados](#)
- [EC2 Las subredes \[EC2.44\] deben estar etiquetadas](#)
- [\[EC2.45\] los EC2 volúmenes deben estar etiquetados](#)
- [\[EC2.46\] Amazon VPCs debería estar etiquetado](#)
- [\[EC2.47\] Los servicios de puntos de conexión de Amazon VPC deben etiquetarse](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben etiquetarse](#)
- [\[EC2.49\] Las conexiones de emparejamiento de Amazon VPC deben etiquetarse](#)
- [\[EC2.50\] Las puertas de enlace de EC2 VPN deben etiquetarse](#)
- [\[EC2.52\] Las EC2 puertas de enlace de](#)
- [\[EC2.174\] Los conjuntos de opciones de EC2 DHCP deben estar etiquetados](#)
- [\[EC2.175\] Las plantillas de EC2 lanzamiento deben estar etiquetadas](#)
- [\[EC2.176\] Las listas de EC2 prefijos deben estar etiquetadas](#)
- [\[EC2.177\] las sesiones espejo EC2 de tráfico deberían estar etiquetadas](#)
- [\[EC2.178\] Los filtros espejo de EC2 tráfico deben estar etiquetados](#)
- [\[EC2.179\] Los objetivos EC2 de tráfico reflejados deben estar etiquetados](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[ECS.13\] Los servicios de ECS deben estar etiquetados](#)
- [\[ECS.14\] Los clústeres de ECS deben etiquetarse](#)
- [\[ECS.15\] Las definiciones de tareas de ECS deben etiquetarse](#)
- [\[EFS.5\] Los puntos de acceso de EFS deben etiquetarse](#)
- [\[EKS.6\] Los clústeres de EKS deben etiquetarse](#)
- [\[EKS.7\] Las configuraciones de los proveedores de identidad de EKS deben etiquetarse](#)
- [\[ES.9\] Los dominios de Elasticsearch deben estar etiquetados](#)
- [\[EventBridge.2\] los autobuses de EventBridge eventos deben estar etiquetados](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[Glue.1\] los AWS Glue trabajos deben estar etiquetados](#)

- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[GuardDuty.3\] GuardDuty IPSets debe estar etiquetado](#)
- [\[GuardDuty.4\] GuardDuty los detectores deben estar etiquetados](#)
- [\[IAM.23\] Los analizadores del Analizador de acceso de IAM deben etiquetarse](#)
- [\[IAM.24\] Los roles de IAM deben etiquetarse](#)
- [\[IAM.25\] Los usuarios de IAM deben etiquetarse](#)
- [Los perfiles de AWS IoT Device Defender seguridad \[IoT.1\] deben estar etiquetados](#)
- [\[IoT.2\] las acciones de AWS IoT Core mitigación deben estar etiquetadas](#)
- [AWS IoT Core Las dimensiones de \[IoT.3\] deben estar etiquetadas](#)
- [Los AWS IoT Core autorizadores \[IoT.4\] deben estar etiquetados](#)
- [Los alias de los AWS IoT Core roles \[IoT.5\] deben estar etiquetados](#)
- [AWS IoT Core Las políticas \[IoT.6\] deben estar etiquetadas](#)
- [\[IoTEvents .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoTEvents .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoTEvents .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoTSiteWise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoTSiteWise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[IoT TwinMaker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoT TwinMaker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoT TwinMaker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoT TwinMaker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoT Wireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)

- [\[Keyspaces.1\]](#) Los espacios clave de Amazon Keyspaces deben estar etiquetados
- [\[Kinesis.2\]](#) Las transmisiones de Kinesis deben etiquetarse
- [\[Lambda.6\]](#) Las funciones de Lambda deben estar etiquetadas
- [\[MQ.4\]](#) Los agentes de Amazon MQ deben estar etiquetados
- [Los NetworkFirewall firewalls de Network Firewall se deben etiquetar](#)
- [\[NetworkFirewall.8\]](#) Las políticas de firewall de Network Firewall se deben etiquetar
- [Los OpenSearch dominios \[Opensearch.9\]](#) deben estar etiquetados
- [\[PCA.2\]](#) Se debe etiquetar a las autoridades certificadoras de CA AWS privadas
- [\[RDS.28\]](#) Los clústeres de base de datos de RDS deben etiquetarse
- [\[RDS.29\]](#) Las instantáneas del clúster de base de datos de RDS deben etiquetarse
- [\[RDS.30\]](#) Las instancias de bases de datos de RDS deben etiquetarse
- [\[RDS.31\]](#) Los grupos de seguridad de bases de datos de RDS deben etiquetarse
- [\[RDS.32\]](#) Las instantáneas de bases de datos de RDS deben etiquetarse
- [\[RDS.33\]](#) Los grupos de subredes de bases de datos de RDS deben etiquetarse
- [\[Redshift.11\]](#) Los clústeres de Redshift deben etiquetarse
- [\[Redshift.12\]](#) Las suscripciones a notificaciones de eventos de Redshift deben etiquetarse
- [\[Redshift.13\]](#) Las instantáneas del clúster de Redshift deben etiquetarse
- [\[Redshift.14\]](#) Los grupos de subredes del clúster de Redshift deben etiquetarse
- [\[Redshift.17\]](#) Los grupos de parámetros del clúster de Redshift deben estar etiquetados
- [\[Route53.1\]](#) Las comprobaciones de estado de Route 53 deben estar etiquetadas
- [\[SageMaker.6\]](#) Las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas
- [\[SageMaker.7\]](#) SageMaker las imágenes deben estar etiquetadas
- [\[SecretsManager.5\]](#) Los secretos de Secrets Manager deben estar etiquetados
- [\[SES.1\]](#) Las listas de contactos de SES deben estar etiquetadas
- [\[SES.2\]](#) Los conjuntos de configuración de SES deben estar etiquetados
- [\[SNS.3\]](#) Los temas de SNS deben etiquetarse
- [\[SQS.2\]](#) Las colas de SQS deben estar etiquetadas
- [\[SSM.5\]](#) Los documentos SSM deben estar etiquetados
- [\[StepFunctions.2\]](#) Las actividades de Step Functions deben estar etiquetadas

- [Los AWS Transfer Family flujos de trabajo de \[Transfer.1\] deben estar etiquetados](#)
- [\[Transfer.4\] Los acuerdos Transfer Family deben estar etiquetados](#)
- [\[Transfer.5\] Los certificados de Transfer Family deben estar etiquetados](#)
- [\[Transfer.6\] Los conectores Transfer Family deben estar etiquetados](#)
- [\[Transfer.7\] Los perfiles de Transfer Family deben estar etiquetados](#)

CIS AWS Foundations es el punto de referencia en Security Hub (CSPM)

El Center for Internet Security (CIS) AWS Foundations Benchmark sirve como un conjunto de mejores prácticas de configuración de seguridad para AWS. Estas mejores prácticas aceptadas por la industria le proporcionan procedimientos claros de step-by-step implementación y evaluación. Desde sistemas operativos hasta servicios en la nube y dispositivos de red, los controles de este punto de referencia le ayudan a proteger los sistemas específicos que utiliza su organización.

AWS Security Hub Cloud Security Posture Management (CSPM) es compatible con las versiones 3.0.0, 1.4.0 y 1.2.0 de CIS AWS Foundations Benchmark. En esta página se enumeran los controles de seguridad compatibles con cada versión. También proporciona una comparación de las versiones.

CIS AWS Foundations Benchmark, versión 3.0.0

Security Hub CSPM es compatible con la versión 3.0.0 (v3.0.0) del CIS Foundations Benchmark. AWS Security Hub CSPM ha cumplido con los requisitos de la certificación de software de seguridad CIS y ha recibido la certificación de software de seguridad CIS para los siguientes puntos de referencia de CIS:

- Índice de referencia de la CEI para AWS las bases de datos de la CEI, versión 3.0.0, nivel 1
- Punto de referencia CIS para CIS AWS Foundations Benchmark, v3.0.0, nivel 2

Controles que se aplican a la versión 3.0.0 de CIS AWS Foundations Benchmark

[\[Cuenta.1\] La información de contacto de seguridad debe proporcionarse para un Cuenta de AWS](#)

[\[CloudTrail.1\] CloudTrail debe habilitarse y configurarse con al menos un registro de seguimiento para varias regiones que incluya eventos de administración de lectura y escritura](#)

[\[CloudTrail.2\] CloudTrail debe tener habilitado el cifrado en reposo](#)

[\[CloudTrail.4\] La validación de archivo de CloudTrail registro debe estar habilitada](#)

[\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el bucket de CloudTrail S3](#)

[\[Config.1\] AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos](#)

[\[EC22\] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente](#)

[\[EC2.6\] El registro de flujos de VPC debe estar habilitado en todos VPCs](#)

[\[EC2.7\] El cifrado predeterminado de EBS debe estar activado](#)

[\[EC2.8\] EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancias IMDSv2](#)

[\[EC2.21\] La red no ACLs debe permitir la entrada desde 0.0.0/0 al puerto 22 o al puerto 3389](#)

[\[EC2.53\] Los grupos EC2 de seguridad no deberían permitir la entrada de 0.0.0.0/0 a los puertos de administración de servidores remotos](#)

[\[EC2.54\] Los grupos EC2 de seguridad no deberían permitir la entrada de: :/0 a los puertos de administración de servidores remotos](#)

[\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)

[\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)

[\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)

[\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)

[\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)

[\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)

[\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)

[\[IAM.15\] Asegurar que la política de contraseñas de IAM requiera una longitud mínima de 14 o más](#)

[\[IAM.16\] Asegurar que la política de contraseñas de IAM impida la reutilización de contraseñas](#)

[\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)

[\[IAM.22\] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días](#)

[\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)

[\[IAM.27\] Las identidades de IAM no deben tener adjunta la política AWSCloud ShellFullAccess](#)

[\[IAM.28\] El analizador de acceso externo del Analizador de acceso de IAM debe habilitarse](#)

[La rotación de AWS KMS teclas \[KMS.4\] debe estar habilitada](#)

[\[RDS.2\] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible](#)

[\[RDS.3\] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo](#)

[Las actualizaciones automáticas de las versiones secundarias de RDS \[RDS.13\] deben estar habilitadas](#)

[\[S3.1\] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público](#)

[\[S3.5\] En las solicitudes de los buckets de uso general de S3, se debe pedir el uso de SSL](#)

[\[S3.8\] Los buckets de uso general de S3 deben bloquear el acceso público](#)

[\[S3.20\] Los buckets de uso general de S3 deben tener habilitada la eliminación de MFA](#)

[\[S3.22\] Los buckets de uso general de S3 deben registrar eventos de escritura a nivel de objeto](#)

[\[S3.23\] Los buckets de uso general de S3 deben registrar eventos de lectura a nivel de objeto](#)

CIS AWS Foundations Benchmark, versión 1.4.0

Security Hub CSPM es compatible con la versión 1.4.0 (v1.4.0) del CIS Foundations Benchmark. AWS

Controles que se aplican a la versión 1.4.0 de CIS Foundations Benchmark AWS

[\[CloudTrail.1\] CloudTrail debe habilitarse y configurarse con al menos un registro de seguimiento para varias regiones que incluya eventos de administración de lectura y escritura](#)

[\[CloudTrail.2\] CloudTrail debe tener habilitado el cifrado en reposo](#)

[\[CloudTrail.4\] La validación de archivo de CloudTrail registro debe estar habilitada](#)

[\[CloudTrail.5\] CloudTrail Los senderos deben estar integrados con Amazon Logs CloudWatch](#)

[\[CloudTrail.6\] Asegurar que los CloudTrail registros del bucket de S3 no son de acceso público](#)

[\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el bucket de CloudTrail S3](#)

[\[CloudWatch.1\] Debe existir un filtro de métricas de registro y una alarma para el uso del usuario «raíz»](#)

[\[CloudWatch.4\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de IAM](#)

[\[CloudWatch.5\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de CloudTrail configuración de](#)

[\[CloudWatch.6\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los errores de AWS Management Console autenticación](#)

[\[CloudWatch.7\] Asegurar que haya un filtro de métricas de registro y alarma de registro para la deshabilitación o eliminación programada de claves administradas por el cliente](#)

[\[CloudWatch.8\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de bucket de S3](#)

[\[CloudWatch.9\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de AWS Config configuración de](#)

[\[CloudWatch.10\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de grupos de seguridad](#)

[\[CloudWatch.11\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios en las listas de control de acceso a la red \(NACL\)](#)

[\[CloudWatch.12\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a las puertas de enlace de la red](#)

[\[CloudWatch.13\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a la tabla de enrutamiento](#)

[\[CloudWatch.14\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de VPC](#)

[\[Config.1\] AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos](#)

[\[EC22\] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente](#)

[\[EC2.6\] El registro de flujos de VPC debe estar habilitado en todos VPCs](#)

[\[EC2.7\] El cifrado predeterminado de EBS debe estar activado](#)

[\[EC2.21\] La red no ACLs debe permitir la entrada desde 0.0.0/0 al puerto 22 o al puerto 3389](#)

[\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)

[\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)

[\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)

[\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)

[\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)

[\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)

[\[IAM.15\] Asegurar que la política de contraseñas de IAM requiera una longitud mínima de 14 o más](#)

[\[IAM.16\] Asegurar que la política de contraseñas de IAM impida la reutilización de contraseñas](#)

[\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)

[\[IAM.22\] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días](#)

[La rotación de AWS KMS teclas \[KMS.4\] debe estar habilitada](#)

[\[RDS.3\] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo](#)

[\[S3.1\] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público](#)

[\[S3.5\] En las solicitudes de los buckets de uso general de S3, se debe pedir el uso de SSL](#)

[\[S3.8\] Los buckets de uso general de S3 deben bloquear el acceso público](#)

[\[S3.20\] Los buckets de uso general de S3 deben tener habilitada la eliminación de MFA](#)

CIS AWS Foundations Benchmark, versión 1.2.0

Security Hub CSPM es compatible con la versión 1.2.0 (v1.2.0) del CIS Foundations Benchmark. AWS Security Hub CSPM ha cumplido con los requisitos de la certificación de software de seguridad CIS y ha recibido la certificación de software de seguridad CIS para los siguientes puntos de referencia de CIS:

- Índice de referencia de la CEI para los AWS fundamentos de la CEI, versión 1.2.0, nivel 1
- Punto de referencia CIS para CIS AWS Foundations Benchmark, v1.2.0, nivel 2

Controles que se aplican a la versión 1.2.0 de CIS AWS Foundations Benchmark

[\[CloudTrail.1\] CloudTrail debe habilitarse y configurarse con al menos un registro de seguimiento para varias regiones que incluya eventos de administración de lectura y escritura](#)

[\[CloudTrail.2\] CloudTrail debe tener habilitado el cifrado en reposo](#)

[\[CloudTrail.4\] La validación de archivo de CloudTrail registro debe estar habilitada](#)

[\[CloudTrail.5\] CloudTrail Los senderos deben estar integrados con Amazon Logs CloudWatch](#)

[\[CloudTrail.6\] Asegurar que los CloudTrail registros del bucket de S3 no son de acceso público](#)

[\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el bucket de CloudTrail S3](#)

[\[CloudWatch.1\] Debe existir un filtro de métricas de registro y una alarma para el uso del usuario «raíz»](#)

[\[CloudWatch.2\] Asegurar que haya un filtro de métricas de registro y alarma para las llamadas a la API no autorizadas](#)

[\[CloudWatch.3\] Asegurar que haya un filtro de métricas de registro y alarma de registro para el inicio de sesión en la Consola de administración sin MFA](#)

[\[CloudWatch.4\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de IAM](#)

[\[CloudWatch.5\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de CloudTrail configuración de](#)

[\[CloudWatch.6\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los errores de AWS Management Console autenticación](#)

[\[CloudWatch.7\] Asegurar que haya un filtro de métricas de registro y alarma de registro para la deshabilitación o eliminación programada de claves administradas por el cliente](#)

[\[CloudWatch.8\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de bucket de S3](#)

[\[CloudWatch.9\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de AWS Config configuración de](#)

[\[CloudWatch.10\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de grupos de seguridad](#)

[\[CloudWatch.11\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios en las listas de control de acceso a la red \(NACL\)](#)

[\[CloudWatch.12\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a las puertas de enlace de la red](#)

[\[CloudWatch.13\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a la tabla de enrutamiento](#)

[\[CloudWatch.14\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de VPC](#)

[\[Config.1\] AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos](#)

[\[EC22\] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente](#)

[\[EC2.6\] El registro de flujos de VPC debe estar habilitado en todos VPCs](#)

[\[EC2.13\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0.0.0/0 o: :/0 al puerto 22](#)

[\[EC2.14\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0.0.0/0 o: :/0 al puerto 3389](#)

[\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)

[\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)

[\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)

[\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)

[\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)

[\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)

[\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)

[\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)

[\[IAM.11\] Asegurar que la política de contraseñas de IAM requiera al menos una letra mayúscula](#)

[\[IAM.12\] Asegurar que la política de contraseñas de IAM requiera al menos una letra minúscula](#)

[\[IAM.13\] Asegurar que la política de contraseñas de IAM requiera al menos un símbolo](#)

[\[IAM.14\] Asegurar que la política de contraseñas de IAM requiera al menos un número](#)

[\[IAM.15\] Asegurar que la política de contraseñas de IAM requiera una longitud mínima de 14 o más](#)

[\[IAM.16\] Asegurar que la política de contraseñas de IAM impida la reutilización de contraseñas](#)

[\[IAM.17\] Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos](#)

[\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)

[La rotación de AWS KMS teclas \[KMS.4\] debe estar habilitada](#)

Comparación de versiones de CIS AWS Foundations Benchmark

En esta sección se resumen las diferencias entre las versiones específicas del Center for Internet Security (CIS) AWS Foundations Benchmark: v3.0.0, v1.4.0 y v1.2.0. AWS Security Hub Cloud Security Posture Management (CSPM) es compatible con cada una de estas versiones del CIS AWS Foundations Benchmark. Sin embargo, recomendamos utilizar la versión 3.0.0 para mantenerse al día con las mejores prácticas de seguridad. Puede tener varias versiones del estándar habilitadas al mismo tiempo. Para obtener información sobre los estándares habilitantes, consulte. [Habilitación de un estándar de seguridad](#) Si desea actualizar a la versión 3.0.0, habilítela antes de deshabilitar una versión anterior. De este modo, se evitan brechas en las comprobaciones de seguridad. [Si utiliza la](#)

[integración CSPM de Security Hub AWS Organizations y desea habilitar por lotes la versión 3.0.0 en varias cuentas, le recomendamos que utilice la configuración central.](#)

Asignación de los controles a los requisitos del CIS en cada versión

Comprenda qué controles admite cada versión del CIS AWS Foundations Benchmark.

ID y título de control	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[Cuenta.1] La información de contacto de seguridad debe proporcionarse para un Cuenta de AWS	1.2	1.2	1.18
[CloudTrail.1] CloudTrail debe habilitarse y configurarse con al menos un registro de seguimiento para varias regiones que incluya eventos de administración de lectura y escritura	3.1	3.1	2.1
[CloudTrail.2] CloudTrail debe tener habilitado el cifrado en reposo	3.5	3.7	2.7
[CloudTrail.4] La validación de archivo de CloudTrail registro debe estar habilitada	3.2	3.2	2.2
[CloudTrail.5] CloudTrail Los senderos deben estar integrados con Amazon Logs CloudWatch	No compatible: el CIS eliminó este requisito	3.4	2.4
[CloudTrail.6] Asegurar que los CloudTrail registros del bucket de S3 no son de acceso público	No compatible: el CIS eliminó este requisito	3.3	2.3
[CloudTrail.7] Asegúrese de que el registro de acceso al bucket de	3.4	3.6	2.6

ID y título de control	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
S3 esté habilitado en el bucket de CloudTrail S3			
[CloudWatch.1] Debe existir un filtro de métricas de registro y una alarma para el uso del usuario «raíz»	No compatible: comprobación manual	4.3	3.3
[CloudWatch.2] Asegurar que haya un filtro de métricas de registro y alarma para las llamadas a la API no autorizadas	No compatible: comprobación manual	No compatible: comprobación manual	3.1
[CloudWatch.3] Asegurar que haya un filtro de métricas de registro y alarma de registro para el inicio de sesión en la Consola de administración sin MFA	No compatible: comprobación manual	No compatible: comprobación manual	3.2
[CloudWatch.4] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de IAM	No compatible: comprobación manual	4.4	3.4
[CloudWatch.5] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de CloudTrail configuración de	No compatible: comprobación manual	4.5	3.5
[CloudWatch.6] Asegurar que haya un filtro de métricas de registro y alarma de registro para los errores de AWS Management Console autenticación	No compatible: comprobación manual	4.6	3.6

ID y título de control	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[CloudWatch.7] Asegurar que haya un filtro de métricas de registro y alarma de registro para la deshabilitación o eliminación programada de claves administradas por el cliente	No compatible: comprobación manual	4.7	3.7
[CloudWatch.8] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de bucket de S3	No compatible: comprobación manual	4.8	3.8
[CloudWatch.9] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de AWS Config configuración de	No compatible: comprobación manual	4.9	3.9
[CloudWatch.10] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de grupos de seguridad	No compatible: comprobación manual	4.10	3.10
[CloudWatch.11] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios en las listas de control de acceso a la red (NACL)	No compatible: comprobación manual	4.11	3.11
[CloudWatch.12] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a las puertas de enlace de la red	No compatible: comprobación manual	4.12	3.12

ID y título de control	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[CloudWatch.13] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios ala tabla de enrutamiento	No compatible: comprobación manual	4.13	3.13
[CloudWatch.14] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de VPC	No compatible: comprobación manual	4.14	3.14
[Config.1] AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos	3.3	3.5	2,5
[EC22] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente	5.4	5.3	4.3
[EC2.6] El registro de flujos de VPC debe estar habilitado en todos VPCs	3.7	3.9	2.9
[EC2.7] El cifrado predeterminado de EBS debe estar activado	2.2.1	2.2.1	No compatible
[EC2.8] EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancias IMDSv2	5.6	No admitido	No admitido
[EC2.13] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0.0.0/0 o: :/0 al puerto 22	No compatible: se sustituyó por los requisitos 5.2 y 5.3	No compatible: se sustituyó por los requisitos 5.2 y 5.3	4.1

ID y título de control	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[EC2.14] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 o: :/0 al puerto 3389	No compatible: se sustituyó por los requisitos 5.2 y 5.3	No compatible: se sustituyó por los requisitos 5.2 y 5.3	4.2
[EC2.21] La red no ACLs debe permitir la entrada desde 0.0.0/0 al puerto 22 o al puerto 3389	5.1	5.1	No compatible
[EC2.53] Los grupos EC2 de seguridad no deberían permitir la entrada de 0.0.0.0/0 a los puertos de administración de servidores remotos	5.2	No admitido	No admitido
[EC2.54] Los grupos EC2 de seguridad no deberían permitir la entrada de: :/0 a los puertos de administración de servidores remotos	5.3	No admitido	No admitido
[EFS.1] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS	2.4.1	No admitido	No admitido
[IAM.1] Las políticas de IAM no deben permitir privilegios administrativos completos “*”	No admitido	1.16	1,22
[IAM.2] Los usuarios de IAM no deben tener políticas de IAM asociadas	1.15	No compatible	1.16
[IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos	1.14	1.14	1.4

ID y título de control	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[IAM.4] La clave de acceso del usuario raíz de IAM no debería existir	1.4	1.4	1.12
[IAM.5] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola	1.10	1.10	1.2
[PCI.IAM.6] La MFA de hardware debe estar habilitada para el usuario raíz	1.6	1.6	1.14
[IAM.8] Deben eliminarse las credenciales de usuario de IAM no utilizadas	No se admite: consulte [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días en su lugar	No se admite: consulte [IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días en su lugar	1.3
[IAM.9] La MFA debe estar habilitada para el usuario raíz	1.5	1.5	1.13
[IAM.11] Asegurar que la política de contraseñas de IAM requiera al menos una letra mayúscula	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	1.5
[IAM.12] Asegurar que la política de contraseñas de IAM requiera al menos una letra minúscula	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	1.6

ID y título de control	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[IAM.13] Asegurar que la política de contraseñas de IAM requiera al menos un símbolo	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	1.7
[IAM.14] Asegurar que la política de contraseñas de IAM requiera al menos un número	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	1.8
[IAM.15] Asegurar que la política de contraseñas de IAM requiera una longitud mínima de 14 o más	1.8	1.8	1.9
[IAM.16] Asegurar que la política de contraseñas de IAM impida la reutilización de contraseñas	1.9	1.9	1.10
[IAM.17] Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	1.11
[IAM.18] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support	1,17	1,17	1.2
[IAM.20] Evite el uso del usuario raíz	No compatible: el CIS eliminó este requisito	No compatible: el CIS eliminó este requisito	1.1
[IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días	1.12	1.12	No compatible: el CIS agregó este requisito en versiones posteriores

ID y título de control	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[IAM.26] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse	1.19	No compatible: el CIS agregó este requisito en versiones posteriores	No compatible: el CIS agregó este requisito en versiones posteriores
[IAM.27] Las identidades de IAM no deben tener adjunta la política AWSCloud ShellFullAccess	1.22	No compatible: el CIS agregó este requisito en versiones posteriores	No compatible: el CIS agregó este requisito en versiones posteriores
[IAM.28] El analizador de acceso externo del Analizador de acceso de IAM debe habilitarse	1,20	No compatible: el CIS agregó este requisito en versiones posteriores	No compatible: el CIS agregó este requisito en versiones posteriores
La rotación de AWS KMS teclas [KMS.4] debe estar habilitada	3.6	3.8	2.8
[Macie.1] Amazon Macie debe estar habilitado	No compatible: comprobación manual	No compatible: comprobación manual	No compatible: comprobación manual
[RDS.2] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible	2.3.3	No compatible: el CIS agregó este requisito en versiones posteriores	No compatible: el CIS agregó este requisito en versiones posteriores

ID y título de control	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[RDS.3] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo	2.3.1	2.3.1	No compatible: el CIS agregó este requisito en versiones posteriores
Las actualizaciones automáticas de las versiones secundarias de RDS [RDS.13] deben estar habilitadas	2.3.2	No compatible: el CIS agregó este requisito en versiones posteriores	No compatible: el CIS agregó este requisito en versiones posteriores
[S3.1] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público	2.1.4	2.1.5	No compatible: el CIS agregó este requisito en versiones posteriores
[S3.5] En las solicitudes de los buckets de uso general de S3, se debe pedir el uso de SSL	2.1.1	2.1.2	No compatible: el CIS agregó este requisito en versiones posteriores
[S3.8] Los buckets de uso general de S3 deben bloquear el acceso público	2.1.4	2.1.5	No compatible: el CIS agregó este requisito en versiones posteriores
[S3.20] Los buckets de uso general de S3 deben tener habilitada la eliminación de MFA	2.1.2	2.1.3	No compatible: el CIS agregó este requisito en versiones posteriores

ARNs para los puntos de referencia de la AWS Fundación CIS

Cuando habilita una o más versiones del índice de referencia de CIS AWS Foundations, comienza a recibir los resultados en el formato de búsqueda de AWS seguridad (ASFF). En el ASFF, cada versión utiliza el siguiente nombre de recurso de Amazon (ARN):

CIS AWS Foundations Benchmark, versión 3.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/3.0.0
```

Punto de referencia sobre AWS fundaciones de la CEI v1.4.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/1.4.0
```

Punto de referencia sobre las AWS fundaciones de la CEI, versión

```
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

Puede utilizar el [GetEnabledStandards](#) funcionamiento de la API CSPM de Security Hub para encontrar el ARN de un estándar habilitado.

Los valores anteriores son para `StandardsArn`. Sin embargo, `StandardsSubscriptionArn` hace referencia al recurso de suscripción estándar que Security Hub CSPM crea al suscribirse a un estándar llamando a una [BatchEnableStandards](#) región.

Note

Al habilitar una versión del CIS AWS Foundations Benchmark, Security Hub CSPM puede tardar hasta 18 horas en generar resultados para los controles que utilizan la misma regla AWS Config vinculada a servicios que los controles habilitados en otros estándares habilitados. Para obtener más información sobre el programa para generar resultados de control, consulte [Programación para ejecutar comprobaciones de seguridad](#).

Los campos de resultados serán diferentes si activa los resultados de los controles consolidados. Para obtener información sobre estas diferencias, consulte [Impacto de la consolidación en los campos y valores ASFF](#). Para ver ejemplos de los resultados de los controles, consulte [Muestras de los resultados de los controles](#).

Requisitos de CIS que no se admiten en Security Hub (CSPM)

Como se indica en la tabla anterior, el Security Hub CSPM no admite todos los requisitos de CIS en todas las versiones del CIS AWS Foundations Benchmark. Muchos de los requisitos no compatibles solo se pueden evaluar revisando manualmente el estado de los recursos. AWS

NIST SP 800-53 revisión 5 en Security Hub CSPM

La publicación especial 800-53 del NIST, revisión 5 (NIST SP 800-53 rev. 5) es un marco de ciberseguridad y cumplimiento desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), una agencia que forma parte del Departamento de Comercio de los Estados Unidos. Este marco de cumplimiento proporciona un catálogo de requisitos de seguridad y privacidad para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información y los recursos críticos. Las agencias del gobierno federal de EE. UU. y los contratistas deben cumplir con estos requisitos para proteger sus sistemas y organizaciones. Las organizaciones privadas también pueden utilizar voluntariamente los requisitos como marco orientativo para reducir el riesgo de ciberseguridad. Para obtener más información sobre el marco y sus requisitos, consulte la norma [NIST SP 800-53 Rev. 5](#) en el Centro de recursos de seguridad informática del NIST.

AWS Security Hub Cloud Security Posture Management (CSPM) proporciona controles de seguridad que admiten un subconjunto de los requisitos de la revisión 5 del NIST SP 800-53. Los controles realizan comprobaciones de seguridad automatizadas para determinados recursos. Servicios de AWS Para habilitar y administrar estos controles, puede habilitar el marco NIST SP 800-53 Revision 5 como estándar en Security Hub CSPM. Tenga en cuenta que los controles no son compatibles con los requisitos de la revisión 5 del NIST SP 800-53, que requieren comprobaciones manuales.

A diferencia de otros marcos, el marco de la revisión 5 del NIST SP 800-53 no es prescriptivo sobre cómo deben evaluarse sus requisitos. En cambio, el marco proporciona pautas. En Security Hub CSPM, el estándar NIST SP 800-53 revisión 5 y los controles representan la comprensión del servicio de estas pautas.

Temas

- [Configurar el registro de recursos para los controles que se aplican al estándar](#)
- [Determinar qué controles se aplican a la norma](#)

Configurar el registro de recursos para los controles que se aplican al estándar

Para optimizar la cobertura y la precisión de los hallazgos, es importante habilitar y configurar el registro de recursos AWS Config antes de habilitar el estándar NIST SP 800-53 revisión 5 en AWS Security Hub Cloud Security Posture Management (CSPM). Cuando configure el registro de recursos, asegúrese también de habilitarlo para todos los tipos de AWS recursos que se comprueban mediante los controles que se aplican a la norma. Esto se aplica principalmente a los controles que tienen un tipo de programa activado por cambios. Sin embargo, algunos controles con un tipo de programación periódica también requieren el registro de recursos. Si el registro de recursos no está habilitado o configurado correctamente, es posible que Security Hub CSPM no pueda evaluar los recursos adecuados ni generar resultados precisos para los controles que se aplican al estándar.

Para obtener información sobre cómo Security Hub CSPM utiliza el registro de recursos AWS Config, consulte [Habilitación y configuración AWS Config de Security Hub CSPM](#). Para obtener información sobre cómo configurar el registro de recursos en AWS Config, consulte [Trabajar con el grabador de configuración](#) en la Guía AWS Config para desarrolladores.

En la siguiente tabla se especifican los tipos de recursos que se van a registrar para los controles que se aplican al estándar NIST SP 800-53, revisión 5, en Security Hub CSPM.

Servicio de AWS	Tipos de recurso
Amazon API Gateway	AWS::ApiGateway::Stage , AWS::ApiGatewayV2::Stage
AWS AppSync	AWS::AppSync::GraphQLApi
AWS Backup	AWS::Backup::RecoveryPoint
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS CloudFormation	AWS::CloudFormation::Stack
Amazon CloudFront	AWS::CloudFront::Distribution
Amazon CloudWatch	AWS::CloudWatch::Alarm
AWS CodeBuild	AWS::CodeBuild::Project

Servicio de AWS	Tipos de recurso
AWS Database Migration Service (AWS DMS)	<code>AWS::DMS::Endpoint</code> , <code>AWS::DMS::ReplicationInstance</code> , <code>AWS::DMS::ReplicationTask</code>
Amazon DynamoDB	<code>AWS::DynamoDB::Table</code>
Amazon Elastic Compute Cloud (Amazon EC2)	<code>AWS::EC2::ClientVpnEndpoint</code> , <code>AWS::EC2::EIP</code> , <code>AWS::EC2::Instance</code> , <code>AWS::EC2::LaunchTemplate</code> , <code>AWS::EC2::NetworkAcl</code> , <code>AWS::EC2::NetworkInterface</code> , <code>AWS::EC2::SecurityGroup</code> , <code>AWS::EC2::Subnet</code> , <code>AWS::EC2::TransitGateway</code> , <code>AWS::EC2::VPNConnection</code> , <code>AWS::EC2::Volume</code>
Amazon EC2 Auto Scaling	<code>AWS::AutoScaling::AutoScalingGroup</code> , <code>AWS::AutoScaling::LaunchConfiguration</code>
Amazon Elastic Container Registry (Amazon ECR)	<code>AWS::ECR::Repository</code>
Amazon Elastic Container Service (Amazon ECS)	<code>AWS::ECS::Cluster</code> , <code>AWS::ECS::Service</code> , <code>AWS::ECS::TaskDefinition</code>
Amazon Elastic File System (Amazon EFS)	<code>AWS::EFS::AccessPoint</code>
Amazon Elastic Kubernetes Service (Amazon EKS)	<code>AWS::EKS::Cluster</code>
AWS Elastic Beanstalk	<code>AWS::ElasticBeanstalk::Environment</code>

Servicio de AWS	Tipos de recurso
Elastic Load Balancing	<code>AWS::ElasticLoadBalancing::LoadBalancer</code> , <code>AWS::ElasticLoadBalancingV2::Listener</code> , <code>AWS::ElasticLoadBalancingV2::LoadBalancer</code>
Amazon ElasticSearch	<code>AWS::Elasticsearch::Domain</code>
Amazon EMR	<code>AWS::EMR::SecurityConfiguration</code>
Amazon EventBridge	<code>AWS::Events::Endpoint</code> , <code>AWS::Events::EventBus</code>
AWS Glue	<code>AWS::Glue::Job</code>
AWS Identity and Access Management (IAM)	<code>AWS::IAM::Group</code> , <code>AWS::IAM::Policy</code> , <code>AWS::IAM::Role</code> , <code>AWS::IAM::User</code>
AWS Key Management Service (AWS KMS)	<code>AWS::KMS::Alias</code> , <code>AWS::KMS::Key</code>
Amazon Kinesis	<code>AWS::Kinesis::Stream</code>
AWS Lambda	<code>AWS::Lambda::Function</code>
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	<code>AWS::MSK::Cluster</code>
Amazon MQ	<code>AWS::AmazonMQ::Broker</code>
AWS Network Firewall	<code>AWS::NetworkFirewall::Firewall</code> , <code>AWS::NetworkFirewall::FirewallPolicy</code> , <code>AWS::NetworkFirewall::RuleGroup</code>
OpenSearch Servicio Amazon	<code>AWS::OpenSearch::Domain</code>

Servicio de AWS	Tipos de recurso
Amazon Relational Database Service (Amazon RDS)	<code>AWS::RDS::DBCluster</code> , <code>AWS::RDS::DBClusterSnapshot</code> , <code>AWS::RDS::DBInstance</code> , <code>AWS::RDS::DBSnapshot</code> , <code>AWS::RDS::EventSubscription</code>
Amazon Redshift	<code>AWS::Redshift::Cluster</code> , <code>AWS::Redshift::ClusterSubnetGroup</code>
Amazon Route 53	<code>AWS::Route53::HostedZone</code>
Amazon Simple Storage Service (Amazon S3)	<code>AWS::S3::AccessPoint</code> , <code>AWS::S3::AccountPublicAccessBlock</code> , <code>AWS::S3::Bucket</code>
AWS Service Catalog	<code>AWS::ServiceCatalog::Portfolio</code>
Amazon Simple Notification Service (Amazon SNS)	<code>AWS::SNS::Topic</code>
Amazon Simple Queue Service (Amazon SQS)	<code>AWS::SQS::Queue</code>
Amazon EC2 Systems Manager (SSM)	<code>AWS::SSM::AssociationCompliance</code> , <code>AWS::SSM::ManagedInstanceInventory</code> , <code>AWS::SSM::PatchCompliance</code>
Amazon SageMaker AI	<code>AWS::SageMaker::NotebookInstance</code>
AWS Secrets Manager	<code>AWS::SecretsManager::Secret</code>
AWS Transfer Family	<code>AWS::Transfer::Connector</code>

Servicio de AWS	Tipos de recurso
AWS WAF	AWS::WAF::Rule , AWS::WAF::RuleGroup , AWS::WAF::WebACL , AWS::WAFRegional::Rule , AWS::WAFRegional::RuleGroup , AWS::WAFRegional::WebACL , AWS::WAFv2::RuleGroup , AWS::WAFv2::WebACL

Determinar qué controles se aplican a la norma

La siguiente lista especifica los controles que cumplen con los requisitos del NIST SP 800-53 revisión 5 y que se aplican al estándar NIST SP 800-53 revisión 5 en Security Hub AWS Cloud Security Posture Management (CSPM). Para obtener información detallada sobre los requisitos específicos que admite un control, seleccione el control. A continuación, consulte el campo Requisitos relacionados en los detalles del control. Este campo especifica cada requisito del NIST que admite el control. Si el campo no especifica un requisito concreto del NIST, el control no lo admite.

- [\[Cuenta.1\] La información de contacto de seguridad debe proporcionarse para un Cuenta de AWS](#)
- [\[Account.2\] Cuentas de AWS debe formar parte de una organización AWS Organizations](#)
- [\[ACM.1\] Los certificados importados y emitidos por ACM deben renovarse después de un período de tiempo específico](#)
- [\[APIGateway.1\] El registro de ejecución de WebSocket REST y API de API Gateway debe estar habilitado](#)
- [\[APIGateway.2\] Las etapas de la API de REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend](#)
- [\[APIGateway.3\] Las etapas de la API de REST de API Gateway tener AWS X-Ray habilitado el rastreo](#)
- [\[APIGateway.4\] La API Gateway debe estar asociada a una ACL web de WAF](#)
- [\[APIGateway.5\] Los datos de la caché de la API de REST de API Gateway deben cifrarse en reposo](#)
- [\[APIGateway.8\] Las rutas de API Gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas V2 de API Gateway](#)

- [\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves de API](#)
- [\[AutoScaling.1\] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar las comprobaciones de estado del ELB](#)
- [\[AutoScaling.2\] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad](#)
- [\[AutoScaling.3\] Las configuraciones de lanzamiento de grupos de Auto Scaling deberían configurar las EC2 instancias para que requieran la versión 2 del Servicio de Metadatos de Instancia \(IMDSv2\)](#)
- [\[AutoScaling.5\] EC2 Las instancias de Amazon lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas](#)
- [\[AutoScaling.6\] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad](#)
- [\[AutoScaling.9\] Los grupos de Amazon EC2 Auto Scaling deberían usar las plantillas de EC2 lanzamiento de Amazon](#)
- [\[Backup.1\] Los puntos AWS Backup de recuperación deben cifrarse en reposo](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudTrail.1\] CloudTrail debe habilitarse y configurarse con al menos un registro de seguimiento para varias regiones que incluya eventos de administración de lectura y escritura](#)
- [\[CloudTrail.2\] CloudTrail debe tener habilitado el cifrado en reposo](#)
- [\[CloudTrail.4\] La validación de archivo de CloudTrail registro debe estar habilitada](#)

- [\[CloudTrail.5\] CloudTrail Los senderos deben estar integrados con Amazon Logs CloudWatch](#)
- [\[CloudTrail.10\] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [\[CloudWatch.15\] CloudWatch las alarmas deben tener configuradas acciones específicas](#)
- [\[CloudWatch.16\] Los grupos de CloudWatch registros deben retenerse durante un periodo específico](#)
- [\[CloudWatch.17\] las acciones CloudWatch de alarma deben estar activadas](#)
- [\[CodeBuild.1\] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales](#)
- [\[CodeBuild.2\] Las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro](#)
- [\[CodeBuild.3\] Los registros de CodeBuild S3 deben estar cifrados](#)
- [\[CodeBuild.4\] Los entornos de los CodeBuild proyectos deben tener una duración de registro AWS Config](#)
- [\[Config.1\] AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos](#)
- [\[DataFirehose.1\] Los flujos de entrega de Firehose deben cifrarse en reposo](#)
- [\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)
- [\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)
- [\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado](#)
- [\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)

- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DynamoDB.1\] Las tablas de DynamoDB deberían escalar automáticamente la capacidad en función de la demanda](#)
- [\[DynamoDB.2\] Las tablas de DynamoDB deben tener habilitada la recuperación point-in-time](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.6\] Las tablas de DynamoDB deben tener la protección contra eliminación habilitada](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.1\] Las instantáneas de Amazon EBS no se deben poder restaurar públicamente](#)
- [\[EC22\] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente](#)
- [\[EC2.3\] Los volúmenes de Amazon EBS asociados deben cifrarse en reposo](#)
- [\[EC24\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.6\] El registro de flujos de VPC debe estar habilitado en todos VPCs](#)
- [\[EC2.7\] El cifrado predeterminado de EBS debe estar activado](#)
- [\[EC2.8\] EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancias IMDSv2](#)
- [\[EC2.9\] EC2 Las instancias de Amazon no deben tener una dirección pública IPv4](#)
- [\[EC2.10\] Amazon EC2 debe configurarse para utilizar los puntos de enlace de VPC que se crean para el servicio de Amazon EC2](#)
- [\[EC2.12\] Amazon no utilizado EC2 EIPs debería retirarse](#)
- [\[EC2.13\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0.0.0/0 o ::/0 al puerto 22](#)

- [\[EC215\] EC2 Las subredes de Amazon no deben asignar automáticamente direcciones IP públicas](#)
- [\[EC2.16\] Deben eliminarse las listas de control de acceso a la red no utilizadas](#)
- [\[EC2.17\] EC2 Las instancias de Amazon no deberían usar múltiples ENIs](#)
- [\[EC2.18\] Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados](#)
- [\[EC219\] Los grupos de seguridad no deben permitir el acceso irrestricto a los puertos de alto riesgo](#)
- [\[EC220\] Ambos túneles de VPN de una conexión de AWS Site-to-Site VPN deben estar activos](#)
- [\[EC2.21\] La red no ACLs debe permitir la entrada desde 0.0.0/0 al puerto 22 o al puerto 3389](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.25\] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red](#)
- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad](#)
- [\[EC251\] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)
- [\[EC2.55\] VPCs debe configurarse con un punto final de interfaz para la API ECR](#)
- [\[EC2.56\] VPCs debe configurarse con un punto final de interfaz para Docker Registry](#)
- [\[EC2.57\] VPCs debe configurarse con un punto final de interfaz para Systems Manager](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[ECR.1\] Los repositorios privados del ECR deben tener configurado el escaneo de imágenes](#)
- [\[ECR.2\] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas](#)
- [\[ECR.3\] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida](#)
- [\[ECR.5\] Los repositorios de ECR deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [\[ECS.1\] Las definiciones de tareas de Amazon ECS deben tener modos de red seguros y definiciones de usuario](#)

- [\[ECS.2\] Los servicios de ECS no deberían tener direcciones IP públicas asignadas automáticamente](#)
- [\[ECS.3\] Las definiciones de tareas de ECS no deben compartir el espacio de nombres de los procesos del anfitrión](#)
- [\[ECS.4\] Los contenedores de ECS deben ejecutarse sin privilegios](#)
- [\[ECS.5\] Los contenedores ECS deben limitarse al acceso de solo lectura a los sistemas de archivos raíz](#)
- [\[ECS.8\] Los secretos no deben pasarse como variables de entorno del contenedor](#)
- [\[ECS.9\] Las definiciones de tareas de ECS deben tener una configuración de registro](#)
- [\[ECS.10\] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate](#)
- [\[ECS.12\] Los clústeres de ECS deben usar Container Insights](#)
- [\[ECS.17\] Las definiciones de tareas de ECS no deben utilizar el modo de red host](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] Los volúmenes de Amazon EFS deben estar en los planes de respaldo](#)
- [\[EFS.3\] Los puntos de acceso EFS deben aplicar un directorio raíz](#)
- [\[EFS.4\] Los puntos de acceso EFS deben imponer una identidad de usuario](#)
- [\[EFS.6\] Los destinos de montaje de EFS no deben estar asociados a una subred pública](#)
- [\[EKS.1\] Los puntos de enlace del clúster EKS no deben ser de acceso público](#)
- [\[EKS.2\] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible](#)
- [\[EKS.3\] Los clústeres de EKS deben usar secretos de Kubernetes cifrados](#)
- [\[EKS.8\] Los clústeres de EKS deben tener habilitado el registro de auditoría](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.2\] ElastiCache Los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias](#)
- [\[ElastiCache.3\] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática](#)
- [\[ElastiCache.4\] los grupos de ElastiCache replicación deben estar cifrados en reposo](#)

- [\[ElastiCache.5\] los grupos de ElastiCache replicación deben cifrarse en tránsito](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)
- [\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)
- [\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)
- [\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)
- [\[ELB.1\] El equilibrador de carga de aplicación debe configurarse para redirigir todas las solicitudes HTTP a HTTPS](#)
- [\[ELB.2\] Los equilibradores de carga clásicos con agentes de escucha SSL/HTTPS deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.3\] Los oyentes de Equilibrador de carga clásico deben configurarse con una terminación HTTPS o TLS](#)
- [\[ELB.4\] El equilibrador de carga de aplicación debe configurarse para eliminar los encabezados http no válidos](#)
- [\[ELB.5\] El registro de las aplicaciones y de los equilibradores de carga clásicos debe estar habilitado](#)
- [\[ELB.6\] La protección contra la eliminación de un equilibrador de carga de aplicación, de puerta de enlace y de red debe estar habilitada](#)
- [\[ELB.7\] Los equilibradores de carga clásicos deberían tener habilitado el drenaje de conexiones](#)
- [\[ELB.8\] Los equilibradores de carga clásicos con agentes de escucha SSL deben usar una política de seguridad predefinida que tenga una duración sólida AWS Config](#)
- [\[ELB.9\] Los equilibradores de carga clásicos deberían tener habilitado el equilibrio de carga entre zonas](#)
- [\[ELB.10\] Equilibrador de carga clásico debe abarcar varias zonas de disponibilidad](#)
- [\[ELB.12\] Equilibrador de carga de aplicación debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.13\] Los equilibradores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad](#)
- [\[ELB.14\] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)

- [\[ELB.16\] Los equilibradores de carga de aplicaciones deben estar asociados a una ACL web de AWS WAF](#)
- [\[ELB.17\] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas](#)
- [\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)
- [\[EMR.2\] La configuración de bloqueo del acceso público de Amazon EMR debe estar habilitada](#)
- [\[EMR.3\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo](#)
- [\[EMR.4\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito](#)
- [\[ES.1\] Los dominios de Elasticsearch deben tener habilitado el cifrado en reposo](#)
- [\[ES.2\] Los dominios de Elasticsearch no deben ser de acceso público](#)
- [\[ES.3\] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos](#)
- [\[ES.4\] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros](#)
- [\[ES.5\] Los dominios de Elasticsearch deben tener habilitado el registro de auditoría](#)
- [\[ES.6\] Los dominios de Elasticsearch deben tener al menos tres nodos de datos](#)
- [\[ES.7\] Los dominios de Elasticsearch deben configurarse con al menos tres nodos maestros dedicados](#)
- [\[ES.8\] Las conexiones a dominios de Elasticsearch deben estar cifradas conforme a la política de seguridad TLS más reciente](#)
- [\[EventBridge.3\] Los autobuses de eventos EventBridge personalizados deben incluir una política basada en los recursos](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FSx.1\] en el caso FSx de OpenZFS, los sistemas de archivos deben configurarse para copiar etiquetas en copias de seguridad y volúmenes](#)
- [\[FSx.2\] FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad](#)
- [\[Glue.4\] Los trabajos de AWS Glue Spark deberían ejecutarse en versiones compatibles de AWS Glue](#)
- [\[GuardDuty.1\] GuardDuty debería estar activado](#)
- [\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)

- [\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)
- [\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)
- [\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)
- [\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)
- [\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)
- [\[IAM.7\] Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)
- [\[IAM.19\] MFA se debe habilitar para todos los usuarios de IAM](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones cómodas en los servicios](#)
- [\[Kinesis.1\] Las transmisiones de Kinesis deben cifrarse en reposo](#)
- [\[KMS.1\] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.2\] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.3\] no AWS KMS keys debe eliminarse involuntariamente](#)
- [La rotación de AWS KMS teclas \[KMS.4\] debe estar habilitada](#)
- [\[Lambda.1\] Las políticas de función de Lambda deberían prohibir el acceso público](#)
- [\[Lambda.2\] Las funciones de Lambda deben usar los tiempos de ejecución admitidos](#)
- [\[Lambda.3\] Las funciones de Lambda deben estar en una VPC](#)
- [\[Lambda.5\] Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)
- [\[MSK.1\] Los clústeres de MSK deben cifrarse en tránsito entre los nodos intermediarios](#)
- [\[MSK.2\] Los clústeres de MSK deberían tener configurada una supervisión mejorada](#)
- [\[MQ.2\] Los corredores de ActiveMQ deberían transmitir los registros de auditoría a CloudWatch](#)
- [\[MQ.3\] Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias](#)

- [\[MQ.5\] Los corredores ActiveMQ deben usar el modo de implementación activo/en espera](#)
- [\[MQ.6\] Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres](#)
- [\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [\[Neptune.4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación](#)
- [\[Neptune.5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas](#)
- [\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM](#)
- [\[Neptune.8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas](#)
- [\[Neptune.9\] Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad](#)
- [Los NetworkFirewall firewalls de Network Firewall se deben implementar en varias zonas de disponibilidad](#)
- [\[NetworkFirewall.2\] El registro de Network Firewall debe estar habilitado](#)
- [\[NetworkFirewall.3\] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas](#)
- [\[NetworkFirewall.4\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos](#)
- [\[NetworkFirewall.5\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados](#)
- [El grupo de reglas de Stateless Network Firewall \[NetworkFirewall.6\] no debe estar vacío](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de eliminación](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de cambio de subred](#)
- [Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)

- [Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)
- [Los OpenSearch dominios \[Opensearch.3\] deben cifrar los datos enviados entre nodos](#)
- [El registro de errores de OpenSearch dominio \[Opensearch.4\] en CloudWatch Logs debe estar activado](#)
- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)
- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los OpenSearch dominios \[Opensearch.7\] deben tener habilitado un control de acceso detallado](#)
- [\[Opensearch.8\] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente](#)
- [Los OpenSearch dominios \[Opensearch.10\] deben tener instalada la última actualización de software](#)
- [Los OpenSearch dominios \[Opensearch.11\] deben tener al menos tres nodos principales dedicados](#)
- [La autoridad emisora de certificados AWS Private CA raíz \[PCA.1\] debe estar deshabilitada](#)
- [\[RDS.1\] La instantánea de RDS debe ser privada](#)
- [\[RDS.2\] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible](#)
- [\[RDS.3\] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo](#)
- [Las instantáneas de clústeres y bases de datos de RDS \[RDS.4\] deben cifrarse cuando están inactivas](#)
- [Las instancias de base de datos de RDS \[RDS.5\] deben configurarse con varias zonas de disponibilidad](#)
- [Se debe configurar una supervisión mejorada para las instancias de base de datos de RDS \[RDS.6\]](#)
- [Los clústeres de RDS \[RDS.7\] deben tener habilitada la protección contra la eliminación](#)
- [Las instancias de base de datos de RDS \[RDS.8\] deben tener habilitada la protección contra la eliminación](#)
- [\[RDS.9\] Las instancias de base de datos de RDS deben publicar los registros en Logs CloudWatch](#)
- [La autenticación de IAM \[RDS.10\] debe configurarse para las instancias de RDS](#)
- [Las instancias RDS \[RDS.11\] deben tener habilitadas las copias de seguridad automáticas](#)
- [La autenticación de IAM \[RDS.12\] debe configurarse para los clústeres de RDS](#)

- [Las actualizaciones automáticas de las versiones secundarias de RDS \[RDS.13\] deben estar habilitadas](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [Los clústeres de bases de datos de RDS \[RDS.15\] deben configurarse para varias zonas de disponibilidad](#)
- [Los clústeres de bases de datos de RDS \[RDS.16\] deben configurarse para copiar etiquetas en las instantáneas](#)
- [Las instancias de base de datos de RDS \[RDS.17\] deben configurarse para copiar etiquetas en las instantáneas](#)
- [Las suscripciones de notificación de eventos de RDS \[RDS.19\] existentes deben configurarse para los eventos de clúster críticos](#)
- [Las suscripciones de notificación de eventos de RDS \[RDS.20\] existentes deben configurarse para eventos críticos de instancias de bases de datos](#)
- [Se debe configurar una suscripción a las notificaciones de eventos de RDS \[RDS.21\] para los eventos críticos de los grupos de parámetros de bases de datos](#)
- [Se debe configurar una suscripción a las notificaciones de eventos de RDS \[RDS.22\] para los eventos críticos de los grupos de seguridad de bases de datos](#)
- [Las instancias RDS \[RDS.23\] no deben usar el puerto predeterminado de un motor de base de datos](#)
- [Los clústeres de bases de datos de RDS \[RDS.24\] deben usar un nombre de usuario de administrador personalizado](#)
- [Las instancias de bases de datos de RDS \[RDS.25\] deben usar un nombre de usuario de administrador personalizado](#)
- [Las instancias de base de datos de RDS \[RDS.26\] deben protegerse mediante un plan de copias de seguridad](#)
- [Los clústeres de bases de datos de RDS \[RDS.27\] deben cifrarse en reposo](#)
- [\[RDS.34\] Los clústeres de bases de datos Aurora MySQL deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[RDS.40\] Las instancias de base de datos de RDS para SQL Server deberían publicar los registros en Logs CloudWatch](#)

- [\[RDS.42\] Las instancias de base de datos de RDS para MariaDB deberían publicar registros en Logs CloudWatch](#)
- [\[Redshift.1\] Los clústeres de Amazon Redshift deberían prohibir el acceso público](#)
- [Las conexiones a los clústeres de Amazon Redshift \[Redshift.2\] deben cifrarse en tránsito](#)
- [Los clústeres de Amazon Redshift \[Redshift.3\] deben tener habilitadas las instantáneas automáticas](#)
- [Los clústeres de Amazon Redshift \[Redshift.4\] deben tener habilitado el registro de auditoría](#)
- [Amazon Redshift \[Redshift.6\] debería tener habilitadas las actualizaciones automáticas a las versiones principales](#)
- [Los clústeres de Redshift \[Redshift.7\] deberían utilizar un enrutamiento de VPC mejorado](#)
- [Los clústeres de Amazon Redshift \[Redshift.8\] no deben usar el nombre de usuario de administrador predeterminado](#)
- [Los clústeres de Redshift \[Redshift.9\] no deben usar el nombre de base de datos predeterminado](#)
- [Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo](#)
- [\[RedshiftServerless.4\] Los espacios de nombres de Redshift Serverless deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de base de datos predeterminado](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.1\] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[S3.2\] Los buckets de uso general de S3 deben bloquear el acceso público de lectura](#)
- [\[S3.3\] Los buckets de uso general de S3 deben bloquear el acceso público de escritura](#)
- [\[S3.5\] En las solicitudes de los buckets de uso general de S3, se debe pedir el uso de SSL](#)
- [\[S3.6\] Las políticas de compartimentos de uso general de S3 deberían restringir el acceso a otros Cuentas de AWS](#)
- [\[S3.7\] Los buckets de uso general de S3 deben usar la replicación entre regiones](#)
- [\[S3.8\] Los buckets de uso general de S3 deben bloquear el acceso público](#)
- [\[S3.9\] Los buckets de uso general de S3 deben tener habilitado el registro de acceso al servidor](#)
- [\[S3.10\] Los buckets de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida](#)

- [\[S3.11\] Los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos](#)
- [\[S3.12\] no ACLs debe usarse para administrar el acceso de los usuarios a los depósitos de uso general de S3](#)
- [\[S3.13\] Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida](#)
- [\[S3.14\] Los buckets de uso general de S3 deben tener habilitado el control de versiones](#)
- [\[S3.15\] Los buckets de uso general de S3 deben tener habilitado el bloqueo de objetos](#)
- [\[S3.17\] Los depósitos de uso general de S3 deben cifrarse en reposo con AWS KMS keys](#)
- [\[S3.19\] Los puntos de acceso de S3 deben tener habilitada la configuración de Bloqueo de acceso público](#)
- [\[S3.20\] Los buckets de uso general de S3 deben tener habilitada la eliminación de MFA](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] las instancias de SageMaker notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook](#)
- [\[SageMaker.4\] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1](#)
- [\[SecretsManager.1\] Los secretos de Secrets Manager deberían tener habilitada la rotación automática](#)
- [\[SecretsManager.2\] Los secretos de Secrets Manager configurados con rotación automática deberían rotar correctamente](#)
- [\[SecretsManager.3\] Eliminar los secretos de Secrets Manager no utilizados](#)
- [\[SecretsManager.4\] Los secretos de Secrets Manager deben rotarse en un número específico de días](#)
- [\[ServiceCatalog.1\] Las carteras de Service Catalog solo deben compartirse dentro de una AWS organización](#)
- [\[SNS.1\] Los temas de SNS deben cifrarse en reposo mediante AWS KMS](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SSM.1\] EC2 Las instancias de Amazon deben administrarse mediante AWS Systems Manager](#)
- [\[SSM.2\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de parche de COMPLIANT después de la instalación de un parche](#)

- [\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [\[SSM.4\] Los documentos SSM no deben ser públicos](#)
- [\[Transfer.2\] Los servidores de Transfer Family no deben utilizar el protocolo FTP para la conexión del punto de conexión](#)
- [\[Transfer.3\] Los conectores Transfer Family deben tener habilitado el registro](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas de \[WAF.2\] Regionales AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.4\] Regionales AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [La AWS WAF web de \[WAF.10\] ACLs debe tener al menos una regla o grupo de reglas](#)
- [El registro de ACL AWS WAF web de \[WAF.11\] debe estar habilitado](#)
- [AWS WAF Las reglas de \[WAF.12\] deben tener habilitadas las métricas CloudWatch](#)

NIST SP 800-171 revisión 2 en Security Hub CSPM

La publicación especial 800-171 revisión 2 del NIST (NIST SP 800-171 rev. 2) es un marco de ciberseguridad y cumplimiento desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), una agencia que forma parte del Departamento de Comercio de los Estados Unidos. Este marco de cumplimiento proporciona los requisitos de seguridad recomendados para proteger la confidencialidad de la información no clasificada controlada en sistemas y organizaciones que no forman parte del gobierno federal de los EE. UU. La información no clasificada controlada, también conocida como CUI, es información confidencial que no cumple con los criterios gubernamentales de clasificación, pero que debe protegerse. Se trata de información que se considera confidencial y que ha sido creada o poseída por el gobierno federal de los EE. UU. u otras entidades en nombre del gobierno federal de los EE. UU.

La norma NIST SP 800-171 Rev. 2 establece los requisitos de seguridad recomendados para proteger la confidencialidad de la información confidencial cuando:

- La información reside en sistemas y organizaciones no federales,
- La organización no federal no recopila ni mantiene información en nombre de una agencia federal ni utiliza ni opera un sistema en nombre de una agencia, y
- La ley, el reglamento o la política gubernamental que los autorice no establecen requisitos de salvaguardia específicos para proteger la confidencialidad de la información confidencial de información confidencial prescrita en la legislación, reglamento o política gubernamental que los autorice para la categoría de información confidencial que figura en el registro de información confidencial de información confidencial.

Los requisitos se aplican a todos los componentes de los sistemas y organizaciones no federales que procesan, almacenan o transmiten la CUI, o que proporcionan protección de seguridad a los componentes. Para obtener más información, consulte la norma [NIST SP 800-171 Rev. 2 en el Centro de recursos de seguridad informática del NIST](#).

AWS Security Hub Cloud Security Posture Management (CSPM) proporciona controles de seguridad que admiten un subconjunto de los requisitos del NIST SP 800-171, revisión 2. Los controles realizan comprobaciones de seguridad automatizadas para determinados recursos. Servicios de AWS Para habilitar y administrar estos controles, puede habilitar el marco NIST SP 800-171 Revision 2 como estándar en Security Hub CSPM. Tenga en cuenta que los controles no son compatibles con los requisitos del NIST SP 800-171, revisión 2, que requieren comprobaciones manuales.

Temas

- [Configurar el registro de recursos para los controles que se aplican a la norma](#)
- [Determinar qué controles se aplican a la norma](#)

Configurar el registro de recursos para los controles que se aplican a la norma

Para optimizar la cobertura y la precisión de los hallazgos, es importante habilitar y configurar el registro de recursos AWS Config antes de habilitar el estándar NIST SP 800-171 revisión 2 en AWS Security Hub Cloud Security Posture Management (CSPM). Cuando configure el registro de recursos, asegúrese también de habilitarlo para todos los tipos de AWS recursos que se comprueban mediante los controles que se aplican al estándar. De lo contrario, es posible que Security Hub CSPM no pueda evaluar los recursos adecuados y generar resultados precisos para los controles que se aplican a la norma.

Para obtener información sobre cómo Security Hub CSPM utiliza el registro de recursos AWS Config, consulte. [Habilitación y configuración AWS Config de Security Hub CSPM](#) Para obtener información

sobre cómo configurar el registro de recursos en AWS Config, consulte [Trabajar con el grabador de configuración](#) en la Guía AWS Config para desarrolladores.

En la siguiente tabla se especifican los tipos de recursos que se van a registrar para los controles que se aplican al estándar NIST SP 800-171, revisión 2, en Security Hub CSPM.

Servicio de AWS	Tipos de recurso
AWS Certificate Manager(ACM)	AWS::ACM::Certificate
Amazon API Gateway	AWS::ApiGateway::Stage
Amazon CloudFront	AWS::CloudFront::Distribution
Amazon CloudWatch	AWS::CloudWatch::Alarm
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::ClientVpnEndpoint , AWS::EC2::NetworkAcl , AWS::EC2:: SecurityGroup , AWS::EC2::VPC , AWS::EC2::VPNConnection
Elastic Load Balancing	AWS::ElasticLoadBalancing:: LoadBalancer
AWS Identity and Access Management(IAM)	AWS::IAM::Policy , AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias , AWS::KMS::Key
AWS Network Firewall	AWS::NetworkFirewall::Firew allPolicy , AWS::NetworkFirewa ll::RuleGroup
Amazon Simple Storage Service (Amazon S3)	AWS::S3::Bucket
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic
AWS Systems Manager(SSM)	AWS::SSM::PatchCompliance
AWS WAF	AWS::WAFv2::RuleGroup

Determinar qué controles se aplican a la norma

La siguiente lista especifica los controles que admiten los requisitos del NIST SP 800-171 revisión 2 y que se aplican al estándar NIST SP 800-171 revisión 2 en Security Hub Cloud Security Posture Management AWS (CSPM). Para obtener información sobre los requisitos específicos que admite un control, seleccione el control. A continuación, consulte el campo Requisitos relacionados en los detalles del control. Este campo especifica cada requisito del NIST que admite el control. Si el campo no especifica un requisito concreto del NIST, el control no lo admite.

- [\[ACM.1\] Los certificados importados y emitidos por ACM deben renovarse después de un período de tiempo específico](#)
- [\[APIGateway.2\] Las etapas de la API de REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudTrail.2\] CloudTrail debe tener habilitado el cifrado en reposo](#)
- [\[CloudTrail.3\] Al menos un CloudTrail registro de seguimiento debe habilitarse](#)
- [\[CloudTrail.4\] La validación de archivo de CloudTrail registro debe estar habilitada](#)
- [\[CloudWatch.1\] Debe existir un filtro de métricas de registro y una alarma para el uso del usuario «raíz»](#)
- [\[CloudWatch.2\] Asegurar que haya un filtro de métricas de registro y alarma para las llamadas a la API no autorizadas](#)
- [\[CloudWatch.4\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de IAM](#)
- [\[CloudWatch.5\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de CloudTrail configuración de](#)
- [\[CloudWatch.6\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los errores de AWS Management Console autenticación](#)
- [\[CloudWatch.7\] Asegurar que haya un filtro de métricas de registro y alarma de registro para la deshabilitación o eliminación programada de claves administradas por el cliente](#)
- [\[CloudWatch.8\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de bucket de S3](#)

- [\[CloudWatch.9\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de AWS Config configuración de](#)
- [\[CloudWatch.10\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de grupos de seguridad](#)
- [\[CloudWatch.11\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios en las listas de control de acceso a la red \(NACL\)](#)
- [\[CloudWatch.12\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a las puertas de enlace de la red](#)
- [\[CloudWatch.13\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a la tabla de enrutamiento](#)
- [\[CloudWatch.14\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de VPC](#)
- [\[CloudWatch.15\] CloudWatch las alarmas deben tener configuradas acciones específicas](#)
- [\[EC2.6\] El registro de flujos de VPC debe estar habilitado en todos VPCs](#)
- [\[EC2.10\] Amazon EC2 debe configurarse para utilizar los puntos de enlace de VPC que se crean para el servicio de Amazon EC2](#)
- [\[EC2.13\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 o: :/0 al puerto 22](#)
- [\[EC2.16\] Deben eliminarse las listas de control de acceso a la red no utilizadas](#)
- [\[EC2.18\] Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados](#)
- [\[EC2.19\] Los grupos de seguridad no deben permitir el acceso irrestricto a los puertos de alto riesgo](#)
- [\[EC2.20\] Ambos túneles de VPN de una conexión de AWS Site-to-Site VPN deben estar activos](#)
- [\[EC2.21\] La red no ACLs debe permitir la entrada desde 0.0.0/0 al puerto 22 o al puerto 3389](#)
- [\[EC2.25\] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)
- [\[ELB.2\] Los equilibradores de carga clásicos con agentes de escucha SSL/HTTPS deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.3\] Los oyentes de Equilibrador de carga clásico deben configurarse con una terminación HTTPS o TLS](#)
- [\[ELB.8\] Los equilibradores de carga clásicos con agentes de escucha SSL deben usar una política de seguridad predefinida que tenga una duración sólida AWS Config](#)

- [\[GuardDuty.1\] GuardDuty debería estar activado](#)
- [\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)
- [\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)
- [\[IAM.7\] Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.10\] Las políticas de contraseñas de usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.11\] Asegurar que la política de contraseñas de IAM requiera al menos una letra mayúscula](#)
- [\[IAM.12\] Asegurar que la política de contraseñas de IAM requiera al menos una letra minúscula](#)
- [\[IAM.13\] Asegurar que la política de contraseñas de IAM requiera al menos un símbolo](#)
- [\[IAM.14\] Asegurar que la política de contraseñas de IAM requiera al menos un número](#)
- [\[IAM.15\] Asegurar que la política de contraseñas de IAM requiera una longitud mínima de 14 o más](#)
- [\[IAM.16\] Asegurar que la política de contraseñas de IAM impida la reutilización de contraseñas](#)
- [\[IAM.17\] Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos](#)
- [\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)
- [\[IAM.19\] MFA se debe habilitar para todos los usuarios de IAM](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)
- [\[IAM.22\] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días](#)
- [\[NetworkFirewall.2\] El registro de Network Firewall debe estar habilitado](#)
- [\[NetworkFirewall.3\] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas](#)
- [\[NetworkFirewall.5\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados](#)
- [El grupo de reglas de Stateless Network Firewall \[NetworkFirewall.6\] no debe estar vacío](#)
- [\[S3.5\] En las solicitudes de los buckets de uso general de S3, se debe pedir el uso de SSL](#)
- [\[S3.6\] Las políticas de compartimentos de uso general de S3 deberían restringir el acceso a otros Cuentas de AWS](#)
- [\[S3.9\] Los buckets de uso general de S3 deben tener habilitado el registro de acceso al servidor](#)

- [\[S3.11\] Los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos](#)
- [\[S3.14\] Los buckets de uso general de S3 deben tener habilitado el control de versiones](#)
- [\[S3.17\] Los depósitos de uso general de S3 deben cifrarse en reposo con AWS KMS keys](#)
- [\[SNS.1\] Los temas de SNS deben cifrarse en reposo mediante AWS KMS](#)
- [\[SSM.2\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de parche de COMPLIANT después de la instalación de un parche](#)
- [AWS WAF Las reglas de \[WAF.12\] deben tener habilitadas las métricas CloudWatch](#)

PCI DSS en Security Hub CSPM

El estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) es un marco de cumplimiento externo que proporciona un conjunto de reglas y pautas para el manejo seguro de la información de las tarjetas de crédito y débito. El Consejo de Normas de Seguridad de la PCI (SSC) crea y actualiza este marco.

AWS Security Hub Cloud Security Posture Management (CSPM) proporciona un estándar PCI DSS que puede ayudarlo a cumplir con este marco de terceros. Puede utilizar este estándar para descubrir vulnerabilidades de seguridad en los AWS recursos que gestionan los datos de los titulares de tarjetas. Recomendamos habilitar este estándar cuando dispongas de recursos Cuentas de AWS que almacenen, procesen o transmitan datos del titular de la tarjeta o datos de autenticación confidenciales. Las evaluaciones realizadas por el PCI SSC validaron este estándar.

Security Hub CSPM es compatible con PCI DSS v3.2.1 y PCI DSS v4.0.1. Recomendamos utilizar la versión 4.0.1 para mantenerse al día con las mejores prácticas de seguridad. Puede tener ambas versiones del estándar habilitadas al mismo tiempo. Para obtener información sobre los estándares de activación, consulte [Habilitación de un estándar de seguridad](#). Si actualmente usa la versión 3.2.1 pero solo quiere usar la versión 4.0.1, habilite la versión más reciente antes de deshabilitar la versión anterior. Esto evita brechas en las comprobaciones de seguridad. Si utiliza la integración CSPM de Security Hub AWS Organizations y desea habilitar por lotes la versión 4.0.1 en varias cuentas, le recomendamos que utilice la [configuración central](#) para hacerlo.

En las siguientes secciones se especifican los controles que se aplican a PCI DSS v3.2.1 y PCI DSS v4.0.1.

Controles que se aplican a PCI DSS v3.2.1

La siguiente lista especifica qué controles de AWS Security Hub Cloud Security Posture Management (CSPM) se aplican a PCI DSS v3.2.1. Para revisar los detalles de un control, selecciónelo.

[\[AutoScaling.1\] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar las comprobaciones de estado del ELB](#)

[\[CloudTrail.2\] CloudTrail debe tener habilitado el cifrado en reposo](#)

[\[CloudTrail.3\] Al menos un CloudTrail registro de seguimiento debe habilitarse](#)

[\[CloudTrail.4\] La validación de archivo de CloudTrail registro debe estar habilitada](#)

[\[CloudTrail.5\] CloudTrail Los senderos deben estar integrados con Amazon Logs CloudWatch](#)

[\[CloudWatch.1\] Debe existir un filtro de métricas de registro y una alarma para el uso del usuario «raíz»](#)

[\[CodeBuild.1\] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales](#)

[\[CodeBuild.2\] Las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro](#)

[\[Config.1\] AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos](#)

[\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)

[\[EC2.1\] Las instantáneas de Amazon EBS no se deben poder restaurar públicamente](#)

[\[EC2.2\] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente](#)

[\[EC2.6\] El registro de flujos de VPC debe estar habilitado en todos VPCs](#)

[\[EC2.12\] Amazon no utilizado EC2 EIPs debería retirarse](#)

[\[EC2.13\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 o ::/0 al puerto 22](#)

[\[ELB.1\] El equilibrador de carga de aplicación debe configurarse para redirigir todas las solicitudes HTTP a HTTPS](#)

[\[ES.1\] Los dominios de Elasticsearch deben tener habilitado el cifrado en reposo](#)

[\[ES.2\] Los dominios de Elasticsearch no deben ser de acceso público](#)

[\[GuardDuty.1\] GuardDuty debería estar activado](#)

[\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)

[\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)

[\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)

[\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)

[\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)

[\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)

[\[IAM.10\] Las políticas de contraseñas de usuarios de IAM deben tener configuraciones seguras](#)

[\[IAM.19\] MFA se debe habilitar para todos los usuarios de IAM](#)

[La rotación de AWS KMS teclas \[KMS.4\] debe estar habilitada](#)

[\[Lambda.1\] Las políticas de función de Lambda deberían prohibir el acceso público](#)

[\[Lambda.3\] Las funciones de Lambda deben estar en una VPC](#)

[Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)

[Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)

[\[RDS.1\] La instantánea de RDS debe ser privada](#)

[\[RDS.2\] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible](#)

[\[Redshift.1\] Los clústeres de Amazon Redshift deberían prohibir el acceso público](#)

[\[S3.1\] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público](#)

[\[S3.2\] Los buckets de uso general de S3 deben bloquear el acceso público de lectura](#)

[\[S3.3\] Los buckets de uso general de S3 deben bloquear el acceso público de escritura](#)

[\[S3.5\] En las solicitudes de los buckets de uso general de S3, se debe pedir el uso de SSL](#)

[\[S3.7\] Los buckets de uso general de S3 deben usar la replicación entre regiones](#)

[\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)

[\[SSM.1\] EC2 Las instancias de Amazon deben administrarse mediante AWS Systems Manager](#)

[\[SSM.2\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de parche de COMPLIANT después de la instalación de un parche](#)

[\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)

Controles que se aplican a la versión 4.0.1 de PCI DSS

La siguiente lista especifica qué controles de AWS Security Hub Cloud Security Posture Management (CSPM) se aplican a PCI DSS v4.0.1. Para revisar los detalles de un control, selecciónelo.

[\[ACM.1\] Los certificados importados y emitidos por ACM deben renovarse después de un período de tiempo específico](#)

[\[ACM.2\] Los certificados RSA administrados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)

[\[APIGateway.9\] El registro de acceso debe configurarse para las etapas V2 de API Gateway](#)

[\[AppSync.2\] AWS AppSync debe tener habilitado el registro a nivel de campo](#)

[\[AutoScaling.3\] Las configuraciones de lanzamiento de grupos de Auto Scaling deberían configurar las EC2 instancias para que requieran la versión 2 del Servicio de Metadatos de Instancia \(IMDSv2\)](#)

[\[AutoScaling.5\] EC2 Las instancias de Amazon lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas](#)

[\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)

[\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)

[\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)

[\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)

[\[CloudFront5\] CloudFront las distribuciones deben tener el registro habilitado](#)

[\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)

[\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)

[\[CloudTrail.2\] CloudTrail debe tener habilitado el cifrado en reposo](#)

[\[CloudTrail.3\] Al menos un CloudTrail registro de seguimiento debe habilitarse](#)

[\[CloudTrail.4\] La validación de archivo de CloudTrail registro debe estar habilitada](#)

[\[CloudTrail.6\] Asegurar que los CloudTrail registros del bucket de S3 no son de acceso público](#)

[\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el bucket de CloudTrail S3](#)

[\[CodeBuild.1\] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales](#)

[\[CodeBuild.2\] Las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro](#)

[\[CodeBuild.3\] Los registros de CodeBuild S3 deben estar cifrados](#)

[\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)

[\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)

[\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado](#)

[\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado](#)

[\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias](#)

[\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)

[\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)

[\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)

[\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)

[\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)

[\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)

[\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)

[\[EC2.13\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0.0.0/0 o: :/0 al puerto 22](#)

[\[EC2.14\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0.0.0/0 o: :/0 al puerto 3389](#)

[\[EC215\] EC2 Las subredes de Amazon no deben asignar automáticamente direcciones IP públicas](#)

[\[EC2.16\] Deben eliminarse las listas de control de acceso a la red no utilizadas](#)

[\[EC2.170\] Las plantillas de EC2 lanzamiento deben usar el servicio de metadatos de instancias versión 2 \(\) IMDSv2](#)

[\[EC2.171\] Las conexiones EC2 VPN deben tener el registro habilitado](#)

[\[EC2.21\] La red no ACLs debe permitir la entrada desde 0.0.0/0 al puerto 22 o al puerto 3389](#)

[\[EC2.25\] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red](#)

[\[EC251\] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)

[\[EC2.53\] Los grupos EC2 de seguridad no deberían permitir la entrada de 0.0.0.0/0 a los puertos de administración de servidores remotos](#)

[\[EC2.54\] Los grupos EC2 de seguridad no deberían permitir la entrada de: :/0 a los puertos de administración de servidores remotos](#)

[\[EC2.8\] EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancias IMDSv2](#)

[\[ECR.1\] Los repositorios privados del ECR deben tener configurado el escaneo de imágenes](#)

[\[ECS.10\] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate](#)

[\[ECS.16\] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas](#)

[\[ECS.2\] Los servicios de ECS no deberían tener direcciones IP públicas asignadas automáticamente](#)

[\[ECS.8\] Los secretos no deben pasarse como variables de entorno del contenedor](#)

[\[EFS.4\] Los puntos de acceso EFS deben imponer una identidad de usuario](#)

[\[EKS.1\] Los puntos de enlace del clúster EKS no deben ser de acceso público](#)

[\[EKS.2\] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible](#)

[\[EKS.3\] Los clústeres de EKS deben usar secretos de Kubernetes cifrados](#)

[\[EKS.8\] Los clústeres de EKS deben tener habilitado el registro de auditoría](#)

[\[ElastiCache.2\] ElastiCache Los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias](#)

[\[ElastiCache.5\] los grupos de ElastiCache replicación deben cifrarse en tránsito](#)

[\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)

[\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)

[\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)

[\[ELB.12\] Equilibrador de carga de aplicación debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)

[\[ELB.14\] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)

[\[ELB.3\] Los oyentes de Equilibrador de carga clásico deben configurarse con una terminación HTTPS o TLS](#)

[\[ELB.4\] El equilibrador de carga de aplicación debe configurarse para eliminar los encabezados http no válidos](#)

[\[ELB.8\] Los equilibradores de carga clásicos con agentes de escucha SSL deben usar una política de seguridad predefinida que tenga una duración sólida AWS Config](#)

[\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)

[\[EMR.2\] La configuración de bloqueo del acceso público de Amazon EMR debe estar habilitada](#)

[\[ES.2\] Los dominios de Elasticsearch no deben ser de acceso público](#)

[\[ES.3\] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos](#)

[\[ES.5\] Los dominios de Elasticsearch deben tener habilitado el registro de auditoría](#)

[\[ES.8\] Las conexiones a dominios de Elasticsearch deben estar cifradas conforme a la política de seguridad TLS más reciente](#)

[\[EventBridge.3\] Los autobuses de eventos EventBridge personalizados deben incluir una política basada en los recursos](#)

[\[GuardDuty.1\] GuardDuty debería estar activado](#)

[\[GuardDuty.10\] La protección de GuardDuty S3 debe estar habilitada](#)

[\[GuardDuty.6\] La protección de GuardDuty Lambda debe estar habilitada](#)

[\[GuardDuty.7\] La supervisión en tiempo de ejecución de GuardDuty EKS debe estar habilitada](#)

[\[GuardDuty.9\] La protección de GuardDuty RDS debe estar habilitada](#)

[\[IAM.11\] Asegurar que la política de contraseñas de IAM requiera al menos una letra mayúscula](#)

[\[IAM.12\] Asegurar que la política de contraseñas de IAM requiera al menos una letra minúscula](#)

[\[IAM.13\] Asegurar que la política de contraseñas de IAM requiera al menos un símbolo](#)

[\[IAM.14\] Asegurar que la política de contraseñas de IAM requiera al menos un número](#)

[\[IAM.16\] Asegurar que la política de contraseñas de IAM impida la reutilización de contraseñas](#)

[\[IAM.17\] Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos](#)

[\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)

[\[IAM.19\] MFA se debe habilitar para todos los usuarios de IAM](#)

[\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)

[\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)

[\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)

[\[IAM.7\] Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras](#)

[\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)

[\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)

[\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)

[\[Inspector.2\] El análisis de ECR en Amazon Inspector debe estar habilitado](#)

[\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)

[\[Inspector.4\] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado](#)

[La rotación de AWS KMS teclas \[KMS.4\] debe estar habilitada](#)

[\[Lambda.1\] Las políticas de función de Lambda deberían prohibir el acceso público](#)

[\[Lambda.2\] Las funciones de Lambda deben usar los tiempos de ejecución admitidos](#)

[\[MQ.2\] Los corredores de ActiveMQ deberían transmitir los registros de auditoría a CloudWatch](#)

[\[MQ.3\] Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias](#)

[\[MSK.1\] Los clústeres de MSK deben cifrarse en tránsito entre los nodos intermediarios](#)

[\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)

[\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)

[\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)

[Los OpenSearch dominios \[Opensearch.10\] deben tener instalada la última actualización de software](#)

[Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)

[Las actualizaciones automáticas de las versiones secundarias de RDS \[RDS.13\] deben estar habilitadas](#)

[\[RDS.2\] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible](#)

[Las suscripciones de notificación de eventos de RDS \[RDS.20\] existentes deben configurarse para eventos críticos de instancias de bases de datos](#)

[Se debe configurar una suscripción a las notificaciones de eventos de RDS \[RDS.21\] para los eventos críticos de los grupos de parámetros de bases de datos](#)

[Se debe configurar una suscripción a las notificaciones de eventos de RDS \[RDS.22\] para los eventos críticos de los grupos de seguridad de bases de datos](#)

[Los clústeres de bases de datos de RDS \[RDS.24\] deben usar un nombre de usuario de administrador personalizado](#)

[Las instancias de bases de datos de RDS \[RDS.25\] deben usar un nombre de usuario de administrador personalizado](#)

[\[RDS.34\] Los clústeres de bases de datos Aurora MySQL deberían publicar los registros de auditoría en Logs CloudWatch](#)

[Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)

[\[RDS.36\] Las instancias de base de datos de RDS para PostgreSQL deben publicar registros en Logs CloudWatch](#)

[\[RDS.37\] Los clústeres de bases de datos Aurora PostgreSQL deberían publicar registros en Logs CloudWatch](#)

[\[RDS.9\] Las instancias de base de datos de RDS deben publicar los registros en Logs CloudWatch](#)

[\[Redshift.1\] Los clústeres de Amazon Redshift deberían prohibir el acceso público](#)

[\[Redshift.15\] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos](#)

[Las conexiones a los clústeres de Amazon Redshift \[Redshift.2\] deben cifrarse en tránsito](#)

[Los clústeres de Amazon Redshift \[Redshift.4\] deben tener habilitado el registro de auditoría](#)

[Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)

[\[S3.1\] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público](#)

[\[S3.15\] Los buckets de uso general de S3 deben tener habilitado el bloqueo de objetos](#)

[\[S3.17\] Los depósitos de uso general de S3 deben cifrarse en reposo con AWS KMS keys](#)

[\[S3.19\] Los puntos de acceso de S3 deben tener habilitada la configuración de Bloqueo de acceso público](#)

[\[S3.22\] Los buckets de uso general de S3 deben registrar eventos de escritura a nivel de objeto](#)

[\[S3.23\] Los buckets de uso general de S3 deben registrar eventos de lectura a nivel de objeto](#)

[\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)

[\[S3.5\] En las solicitudes de los buckets de uso general de S3, se debe pedir el uso de SSL](#)

[\[S3.8\] Los buckets de uso general de S3 deben bloquear el acceso público](#)

[\[S3.9\] Los buckets de uso general de S3 deben tener habilitado el registro de acceso al servidor](#)

[\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)

[\[SecretsManager.1\] Los secretos de Secrets Manager deberían tener habilitada la rotación automática](#)

[\[SecretsManager.2\] Los secretos de Secrets Manager configurados con rotación automática deberían rotar correctamente](#)

[\[SecretsManager.4\] Los secretos de Secrets Manager deben rotarse en un número específico de días](#)

[\[SSM.2\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de parche de COMPLIANT después de la instalación de un parche](#)

[\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)

[\[StepFunctions.1\] Las máquinas de estado de Step Functions deberían tener el registro activado](#)

[\[Transfer.2\] Los servidores de Transfer Family no deben utilizar el protocolo FTP para la conexión del punto de conexión](#)

[El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)

[El registro de ACL AWS WAF web de \[WAF.11\] debe estar habilitado](#)

Estándares gestionados por servicios en Security Hub CSPM

Un estándar administrado por servicios es un estándar de seguridad que otro Servicio de AWS administra, pero que puede ver en Security Hub CSPM. Por ejemplo, un estándar gestionado por [servicios: AWS Control Tower es un estándar gestionado](#) por servicios que gestiona. AWS Control Tower Un estándar gestionado por servicios se diferencia de un estándar de seguridad que AWS Security Hub Cloud Security Posture Management (CSPM) gestiona de las siguientes maneras:

- Creación y eliminación de estándares: puede crear y eliminar un estándar de administración de servicios con la consola o la API del servicio de administración, o con AWS CLI. Hasta que no cree el estándar en el servicio de administración de una de esas formas, el estándar no aparece en la

consola CSPM de Security Hub y no se puede acceder a él mediante la API CSPM de Security Hub o. AWS CLI

- Sin activación automática de los controles: al crear un estándar gestionado por un servicio, Security Hub CSPM y el servicio de gestión no habilitan automáticamente los controles que se aplican al estándar. Además, cuando Security Hub CSPM lanza nuevos controles para el estándar, estos no se activan automáticamente. Esto supone una desviación de los estándares que gestiona Security Hub CSPM. Para obtener más información sobre la forma habitual de configurar los controles en Security Hub CSPM, consulte. [Descripción de los controles de seguridad en Security Hub CSPM](#)
- Habilitar y deshabilitar los controles: se recomienda habilitar y deshabilitar los controles en el servicio de administración para evitar desviaciones.
- Disponibilidad de los controles: el servicio de administración elige qué controles están disponibles como parte del estándar de administración del servicio. Los controles disponibles pueden incluir todos o un subconjunto de los controles CSPM de Security Hub existentes.

Una vez que el servicio de gestión haya creado el estándar gestionado por el servicio y haya puesto los controles a su disposición, podrá acceder a sus resultados de control, estados de control y puntuación de seguridad estándar en la consola CSPM de Security Hub, en la API CSPM de Security Hub o. AWS CLI Es posible que parte o toda esta información también esté disponible en el servicio de administración.

Seleccione un estándar gestionado por el servicio de la siguiente lista para ver más detalles al respecto.

Estándar de gestión de servicios

- [Estándar gestionado por el servicio: AWS Control Tower](#)

Estándar gestionado por el servicio: AWS Control Tower

Esta sección proporciona información sobre Service-Managed Standard:.. AWS Control Tower

¿Qué es Service-Managed Standard:? AWS Control Tower

Este estándar está diseñado para los usuarios de AWS Security Hub Cloud Security Posture Management (CSPM) y. AWS Control Tower Le permite configurar los controles proactivos AWS Control Tower junto con los controles de detección del Security Hub CSPM en el AWS Control Tower servicio.

Los controles proactivos ayudan a garantizar el cumplimiento de las Cuentas de AWS normas, ya que detectan las acciones que pueden dar lugar a infracciones de las políticas o a errores de configuración. Los controles de Detective detectan el incumplimiento de los recursos (por ejemplo, errores de configuración) dentro de su Cuentas de AWS. Al habilitar controles proactivos y de detección para su AWS entorno, puede mejorar su postura de seguridad en las diferentes etapas del desarrollo.

 Tip

Los estándares gestionados por servicios difieren de los estándares que gestiona AWS Security Hub Cloud Security Posture Management (CSPM). Por ejemplo, debe crear y eliminar un estándar administrado por un servicio en el servicio de administración. Para obtener más información, consulte [Estándares gestionados por servicios en Security Hub CSPM](#).

En la consola y la API de CSPM de Security Hub, puede ver Service-Managed Standard: junto con otros estándares CSPM AWS Control Tower de Security Hub.

Creación del estándar

Este estándar solo está disponible si lo crea en. AWS Control Tower AWS Control Tower crea el estándar cuando se habilita por primera vez un control aplicable mediante uno de los métodos siguientes:

- AWS Control Tower consola
- AWS Control Tower API (llame a la [EnableControl](#)API)
- AWS CLI (ejecuta el [enable-control](#)comando)

Los controles CSPM de Security Hub se identifican en la AWS Control Tower consola como SH. *ControlID*(por ejemplo, SH. CodeBuild.1).

Al crear el estándar, si aún no ha activado Security Hub CSPM, AWS Control Tower también habilita Security Hub CSPM por usted.

Si no lo has configurado AWS Control Tower, no podrás ver ni acceder a este estándar en la consola CSPM de Security Hub, en la API CSPM de Security Hub o. AWS CLI Incluso si lo ha configurado AWS Control Tower, no podrá ver ni acceder a este estándar en Security Hub CSPM sin antes crear el estándar AWS Control Tower mediante uno de los métodos anteriores.

Este estándar solo está disponible en los [Regiones de AWS lugares donde AWS Control Tower está disponible, incluidos](#). AWS GovCloud (US)

Habilitación y deshabilitación de los controles en el estándar

Una vez que haya creado el estándar en la AWS Control Tower consola, podrá ver el estándar y los controles disponibles en ambos servicios.

Una vez que haya creado el estándar por primera vez, no tendrá ningún control que se active automáticamente. Además, cuando Security Hub CSPM agrega nuevos controles, no se habilitan automáticamente para Service-Managed Standard. AWS Control Tower debe activar y desactivar los controles de la entrada estándar AWS Control Tower mediante uno de los siguientes métodos:

- AWS Control Tower consola
- AWS Control Tower API (llame a [EnableControl](#) and [DisableControl](#) APIs)
- AWS CLI (ejecuta los [disable-control](#) comandos [enable-control](#)y)

Al cambiar el estado de activación de un control en AWS Control Tower, el cambio también se refleja en Security Hub CSPM.

Sin embargo, si se desactiva un control en Security Hub CSPM que está activado, se AWS Control Tower produce una desviación del control. El estado del control se muestra como. AWS Control Tower Drifted Puede resolver este problema seleccionando [Volver a registrar la unidad organizativa](#) en la AWS Control Tower consola o desactivando y volviendo a activar el control AWS Control Tower mediante uno de los métodos anteriores.

Si completa las acciones de activación y desactivación, evitará que el control se desvíe. AWS Control Tower

Al activar o desactivar los controles AWS Control Tower, la acción se aplica a todas las cuentas y regiones. Si habilita y deshabilita los controles en Security Hub CSPM (no se recomienda para esta norma), la acción solo se aplica a la cuenta corriente y a la región.

 Note

[La configuración central](#) no se puede usar para administrar Service-Managed Standard. AWS Control Tower Si usa la configuración central, solo puede usar el AWS Control Tower servicio para habilitar y deshabilitar los controles de este estándar para una cuenta administrada centralmente.

Visualización del estado de activación y el estado de control

Puede ver el estado de habilitación de un control mediante uno de los métodos siguientes:

- Consola CSPM de Security Hub, API CSPM de Security Hub o AWS CLI
- AWS Control Tower consola
- AWS Control Tower API para ver una lista de los controles habilitados (llame a la [ListEnabledControlsAPI](#))
- AWS CLI para ver una lista de los controles habilitados (ejecuta el [list-enabled-controls](#) comando)

Un control que se deshabilita AWS Control Tower tiene un estado de activación Disabled en Security Hub CSPM, a menos que se habilite explícitamente ese control en Security Hub CSPM.

Security Hub CSPM calcula el estado del control en función del estado del flujo de trabajo y el estado de conformidad de los resultados del control. Para obtener más información sobre el estado de activación y el estado de control, consulte [Revisión de los detalles de los controles en Security Hub \(CSPM\)](#).

En función de los estados de control, Security Hub CSPM calcula una [puntuación de seguridad](#) para Service-Managed Standard: AWS Control Tower. Esta puntuación solo está disponible en Security Hub CSPM. Además, solo puede ver los [resultados de control](#) en Security Hub CSPM. La puntuación de seguridad y los resultados de control estándar no están disponibles en AWS Control Tower.

Note

Al habilitar los controles para Service-Managed Standard: AWS Control Tower, Security Hub CSPM puede tardar hasta 18 horas en generar los resultados de los controles que utilizan una regla vinculada a un servicio existente. AWS Config Es posible que ya tenga reglas vinculadas a servicios si ha activado otros estándares y controles en Security Hub CSPM. Para obtener más información, consulte [Programación para ejecutar comprobaciones de seguridad](#).

Eliminación de la norma

Puede eliminar este estándar deshabilitando todos los controles aplicables AWS Control Tower mediante uno de los siguientes métodos:

- AWS Control Tower consola
- AWS Control Tower API (llame a la [DisableControlAPI](#))
- AWS CLI (ejecuta el [disable-control](#) comando)

Al deshabilitar todos los controles, se elimina el estándar en todas las cuentas administradas y regiones gobernadas de AWS Control Tower. Al eliminar el estándar, se AWS Control Tower elimina de la página de estándares de la consola CSPM de Security Hub y ya no se puede acceder a él mediante la API CSPM de Security Hub o. AWS CLI

 Note

La desactivación de todos los controles del estándar en Security Hub CSPM no desactiva ni elimina el estándar.

Al deshabilitar el servicio CSPM de Security Hub, se elimina Service-Managed Standard: AWS Control Tower y cualquier otro estándar que haya activado.

Búsqueda del formato de campo para Service-Managed Standard: AWS Control Tower

Cuando cree Service-Managed Standard: AWS Control Tower y habilite los controles para él, empezará a recibir los resultados de control en Security Hub CSPM. Security Hub CSPM informa de los hallazgos de control en el. [AWS Formato de búsqueda de seguridad \(ASFF\)](#) Estos son los valores ASFF del nombre de recurso de Amazon (ARN) de este estándar y GeneratorId:

- ARN estándar — `arn:aws:us-east-1:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0`
- GeneratorId – `service-managed-aws-control-tower/v/1.0.0/CodeBuild.1`

Para ver un ejemplo de hallazgo de Service-Managed Standard:, consulte. AWS Control Tower [Muestras de los resultados de los controles](#)

Controles que se aplican a Service-Managed Standard: AWS Control Tower

Estándar gestionado por el servicio: AWS Control Tower admite un subconjunto de controles que forman parte del estándar de mejores prácticas de seguridad AWS fundamentales (FSBP). Elija un control para ver información al respecto, incluidos los pasos para corregir los errores detectados.

La siguiente lista muestra los controles disponibles para Service-Managed Standard: AWS Control Tower. Los límites Regionales de los controles coinciden con los límites Regionales de los controles corolarios del estándar FSBP. Esta lista muestra el control de seguridad independiente del estándar. IDs En la AWS Control Tower consola, los controles IDs tienen el formato SH. **ControlID**(por ejemplo SH. CodeBuild.1). En Security Hub CSPM, si los [hallazgos de control consolidados](#) están desactivados en su cuenta, el ProductFields.ControlId campo utiliza el ID de control basado en estándares. El ID de control basado en estándares tiene el formato CT. **ControlId**(por ejemplo, CT. CodeBuild.1).

- [\[Cuenta.1\] La información de contacto de seguridad debe proporcionarse para un Cuenta de AWS](#)
- [\[ACM.1\] Los certificados importados y emitidos por ACM deben renovarse después de un período de tiempo específico](#)
- [\[ACM.2\] Los certificados RSA administrados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)
- [\[APIGateway.1\] El registro de ejecución de WebSocket REST y API de API Gateway debe estar habilitado](#)
- [\[APIGateway.2\] Las etapas de la API de REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend](#)
- [\[APIGateway.3\] Las etapas de la API de REST de API Gateway tener AWS X-Ray habilitado el rastreo](#)
- [\[APIGateway.4\] La API Gateway debe estar asociada a una ACL web de WAF](#)
- [\[APIGateway.5\] Los datos de la caché de la API de REST de API Gateway deben cifrarse en reposo](#)
- [\[APIGateway.8\] Las rutas de API Gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas V2 de API Gateway](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves de API](#)
- [\[AutoScaling.1\] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar las comprobaciones de estado del ELB](#)
- [\[AutoScaling.2\] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad](#)
- [\[AutoScaling.3\] Las configuraciones de lanzamiento de grupos de Auto Scaling deberían configurar las EC2 instancias para que requieran la versión 2 del Servicio de Metadatos de Instancia \(IMDSv2\)](#)
- [\[AutoScaling.5\] EC2 Las instancias de Amazon lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas](#)

- [\[AutoScaling.6\] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad](#)
- [\[AutoScaling.9\] Los grupos de Amazon EC2 Auto Scaling deberían usar las plantillas de EC2 lanzamiento de Amazon](#)
- [\[CloudTrail.1\] CloudTrail debe habilitarse y configurarse con al menos un registro de seguimiento para varias regiones que incluya eventos de administración de lectura y escritura](#)
- [\[CloudTrail.2\] CloudTrail debe tener habilitado el cifrado en reposo](#)
- [\[CloudTrail.4\] La validación de archivo de CloudTrail registro debe estar habilitada](#)
- [\[CloudTrail.5\] CloudTrail Los senderos deben estar integrados con Amazon Logs CloudWatch](#)
- [\[CloudTrail.6\] Asegurar que los CloudTrail registros del bucket de S3 no son de acceso público](#)
- [\[CodeBuild.1\] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales](#)
- [\[CodeBuild.2\] Las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro](#)
- [\[CodeBuild.3\] Los registros de CodeBuild S3 deben estar cifrados](#)
- [\[CodeBuild.4\] Los entornos de los CodeBuild proyectos deben tener una duración de registro AWS Config](#)
- [\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)
- [\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDB.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDB.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DynamoDB.1\] Las tablas de DynamoDB deberían escalar automáticamente la capacidad en función de la demanda](#)
- [\[DynamoDB.2\] Las tablas de DynamoDB deben tener habilitada la recuperación point-in-time](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[EC2.1\] Las instantáneas de Amazon EBS no se deben poder restaurar públicamente](#)
- [\[EC2.2\] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente](#)
- [\[EC2.3\] Los volúmenes de Amazon EBS asociados deben cifrarse en reposo](#)

- [\[EC24\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.6\] El registro de flujos de VPC debe estar habilitado en todos VPCs](#)
- [\[EC2.7\] El cifrado predeterminado de EBS debe estar activado](#)
- [\[EC2.8\] EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancias IMDSv2](#)
- [\[EC2.9\] EC2 Las instancias de Amazon no deben tener una dirección pública IPv4](#)
- [\[EC2.10\] Amazon EC2 debe configurarse para utilizar los puntos de enlace de VPC que se crean para el servicio de Amazon EC2](#)
- [\[EC215\] EC2 Las subredes de Amazon no deben asignar automáticamente direcciones IP públicas](#)
- [\[EC2.16\] Deben eliminarse las listas de control de acceso a la red no utilizadas](#)
- [\[EC2.17\] EC2 Las instancias de Amazon no deberían usar múltiples ENIs](#)
- [\[EC2.18\] Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados](#)
- [\[EC219\] Los grupos de seguridad no deben permitir el acceso irrestricto a los puertos de alto riesgo](#)
- [\[EC220\] Ambos túneles de VPN de una conexión de AWS Site-to-Site VPN deben estar activos](#)
- [\[EC2.21\] La red no ACLs debe permitir la entrada desde 0.0.0/0 al puerto 22 o al puerto 3389](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC2.25\] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red](#)
- [\[ECR.1\] Los repositorios privados del ECR deben tener configurado el escaneo de imágenes](#)
- [\[ECR.2\] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas](#)
- [\[ECR.3\] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida](#)
- [\[ECS.1\] Las definiciones de tareas de Amazon ECS deben tener modos de red seguros y definiciones de usuario](#)
- [\[ECS.2\] Los servicios de ECS no deberían tener direcciones IP públicas asignadas automáticamente](#)
- [\[ECS.3\] Las definiciones de tareas de ECS no deben compartir el espacio de nombres de los procesos del anfitrión](#)

- [\[ECS.4\] Los contenedores de ECS deben ejecutarse sin privilegios](#)
- [\[ECS.5\] Los contenedores ECS deben limitarse al acceso de solo lectura a los sistemas de archivos raíz](#)
- [\[ECS.8\] Los secretos no deben pasarse como variables de entorno del contenedor](#)
- [\[ECS.10\] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate](#)
- [\[ECS.12\] Los clústeres de ECS deben usar Container Insights](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] Los volúmenes de Amazon EFS deben estar en los planes de respaldo](#)
- [\[EFS.3\] Los puntos de acceso EFS deben aplicar un directorio raíz](#)
- [\[EFS.4\] Los puntos de acceso EFS deben imponer una identidad de usuario](#)
- [\[EKS.1\] Los puntos de enlace del clúster EKS no deben ser de acceso público](#)
- [\[EKS.2\] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible](#)
- [\[ElastiCache.3\] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática](#)
- [\[ElastiCache.4\] los grupos de ElastiCache replicación deben estar cifrados en reposo](#)
- [\[ElastiCache.5\] los grupos de ElastiCache replicación deben cifrarse en tránsito](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)
- [\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)
- [\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)
- [\[ELB.1\] El equilibrador de carga de aplicación debe configurarse para redirigir todas las solicitudes HTTP a HTTPS](#)
- [\[ELB.2\] Los equilibradores de carga clásicos con agentes de escucha SSL/HTTPS deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.3\] Los oyentes de Equilibrador de carga clásico deben configurarse con una terminación HTTPS o TLS](#)
- [\[ELB.4\] El equilibrador de carga de aplicación debe configurarse para eliminar los encabezados http no válidos](#)

- [\[ELB.5\] El registro de las aplicaciones y de los equilibradores de carga clásicos debe estar habilitado](#)
- [\[ELB.6\] La protección contra la eliminación de un equilibrador de carga de aplicación, de puerta de enlace y de red debe estar habilitada](#)
- [\[ELB.7\] Los equilibradores de carga clásicos deberían tener habilitado el drenaje de conexiones](#)
- [\[ELB.8\] Los equilibradores de carga clásicos con agentes de escucha SSL deben usar una política de seguridad predefinida que tenga una duración sólida AWS Config](#)
- [\[ELB.9\] Los equilibradores de carga clásicos deberían tener habilitado el equilibrio de carga entre zonas](#)
- [\[ELB.10\] Equilibrador de carga clásico debe abarcar varias zonas de disponibilidad](#)
- [\[ELB.12\] Equilibrador de carga de aplicación debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.13\] Los equilibradores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad](#)
- [\[ELB.14\] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)
- [\[ES.1\] Los dominios de Elasticsearch deben tener habilitado el cifrado en reposo](#)
- [\[ES.2\] Los dominios de Elasticsearch no deben ser de acceso público](#)
- [\[ES.3\] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos](#)
- [\[ES.4\] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros](#)
- [\[ES.5\] Los dominios de Elasticsearch deben tener habilitado el registro de auditoría](#)
- [\[ES.6\] Los dominios de Elasticsearch deben tener al menos tres nodos de datos](#)
- [\[ES.7\] Los dominios de Elasticsearch deben configurarse con al menos tres nodos maestros dedicados](#)
- [\[ES.8\] Las conexiones a dominios de Elasticsearch deben estar cifradas conforme a la política de seguridad TLS más reciente](#)
- [\[EventBridge.3\] Los autobuses de eventos EventBridge personalizados deben incluir una política basada en los recursos](#)
- [\[GuardDuty.1\] GuardDuty debería estar activado](#)
- [\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)

- [\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)
- [\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)
- [\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)
- [\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)
- [\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)
- [\[IAM.7\] Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)
- [\[Kinesis.1\] Las transmisiones de Kinesis deben cifrarse en reposo](#)
- [\[KMS.1\] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.2\] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.3\] no AWS KMS keys debe eliminarse involuntariamente](#)
- [La rotación de AWS KMS teclas \[KMS.4\] debe estar habilitada](#)
- [\[Lambda.1\] Las políticas de función de Lambda deberían prohibir el acceso público](#)
- [\[Lambda.2\] Las funciones de Lambda deben usar los tiempos de ejecución admitidos](#)
- [\[Lambda.3\] Las funciones de Lambda deben estar en una VPC](#)
- [\[Lambda.5\] Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad](#)
- [\[MSK.1\] Los clústeres de MSK deben cifrarse en tránsito entre los nodos intermediarios](#)
- [\[MQ.5\] Los corredores ActiveMQ deben usar el modo de implementación activo/en espera](#)
- [\[MQ.6\] Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres](#)
- [\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [\[Neptune.4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación](#)
- [\[Neptune.5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas](#)

- [\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM](#)
- [\[Neptune.8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas](#)
- [\[NetworkFirewall.3\] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas](#)
- [\[NetworkFirewall.4\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos](#)
- [\[NetworkFirewall.5\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados](#)
- [El grupo de reglas de Stateless Network Firewall \[NetworkFirewall.6\] no debe estar vacío](#)
- [Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)
- [Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)
- [Los OpenSearch dominios \[Opensearch.3\] deben cifrar los datos enviados entre nodos](#)
- [El registro de errores de OpenSearch dominio \[Opensearch.4\] en CloudWatch Logs debe estar activado](#)
- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)
- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los OpenSearch dominios \[Opensearch.7\] deben tener habilitado un control de acceso detallado](#)
- [\[Opensearch.8\] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente](#)
- [\[RDS.1\] La instantánea de RDS debe ser privada](#)
- [\[RDS.2\] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible](#)
- [\[RDS.3\] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo](#)
- [Las instantáneas de clústeres y bases de datos de RDS \[RDS.4\] deben cifrarse cuando están inactivas](#)
- [Las instancias de base de datos de RDS \[RDS.5\] deben configurarse con varias zonas de disponibilidad](#)
- [Se debe configurar una supervisión mejorada para las instancias de base de datos de RDS \[RDS.6\]](#)

- [Las instancias de base de datos de RDS \[RDS.8\] deben tener habilitada la protección contra la eliminación](#)
- [\[RDS.9\] Las instancias de base de datos de RDS deben publicar los registros en Logs CloudWatch](#)
- [La autenticación de IAM \[RDS.10\] debe configurarse para las instancias de RDS](#)
- [Las instancias RDS \[RDS.11\] deben tener habilitadas las copias de seguridad automáticas](#)
- [La autenticación de IAM \[RDS.12\] debe configurarse para los clústeres de RDS](#)
- [Las actualizaciones automáticas de las versiones secundarias de RDS \[RDS.13\] deben estar habilitadas](#)
- [Los clústeres de bases de datos de RDS \[RDS.15\] deben configurarse para varias zonas de disponibilidad](#)
- [Las instancias de base de datos de RDS \[RDS.17\] deben configurarse para copiar etiquetas en las instantáneas](#)
- [Las instancias de RDS \[RDS.18\] deben implementarse en una VPC](#)
- [Las suscripciones de notificación de eventos de RDS \[RDS.19\] existentes deben configurarse para los eventos de clúster críticos](#)
- [Las suscripciones de notificación de eventos de RDS \[RDS.20\] existentes deben configurarse para eventos críticos de instancias de bases de datos](#)
- [Se debe configurar una suscripción a las notificaciones de eventos de RDS \[RDS.21\] para los eventos críticos de los grupos de parámetros de bases de datos](#)
- [Se debe configurar una suscripción a las notificaciones de eventos de RDS \[RDS.22\] para los eventos críticos de los grupos de seguridad de bases de datos](#)
- [Las instancias RDS \[RDS.23\] no deben usar el puerto predeterminado de un motor de base de datos](#)
- [Las instancias de bases de datos de RDS \[RDS.25\] deben usar un nombre de usuario de administrador personalizado](#)
- [Los clústeres de bases de datos de RDS \[RDS.27\] deben cifrarse en reposo](#)
- [\[Redshift.1\] Los clústeres de Amazon Redshift deberían prohibir el acceso público](#)
- [Las conexiones a los clústeres de Amazon Redshift \[Redshift.2\] deben cifrarse en tránsito](#)
- [Los clústeres de Amazon Redshift \[Redshift.4\] deben tener habilitado el registro de auditoría](#)
- [Amazon Redshift \[Redshift.6\] debería tener habilitadas las actualizaciones automáticas a las versiones principales](#)

- [Los clústeres de Redshift \[Redshift.7\] deberían utilizar un enrutamiento de VPC mejorado](#)
- [Los clústeres de Amazon Redshift \[Redshift.8\] no deben usar el nombre de usuario de administrador predeterminado](#)
- [Los clústeres de Redshift \[Redshift.9\] no deben usar el nombre de base de datos predeterminado](#)
- [Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo](#)
- [\[S3.1\] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[S3.2\] Los buckets de uso general de S3 deben bloquear el acceso público de lectura](#)
- [\[S3.3\] Los buckets de uso general de S3 deben bloquear el acceso público de escritura](#)
- [\[S3.5\] En las solicitudes de los buckets de uso general de S3, se debe pedir el uso de SSL](#)
- [\[S3.6\] Las políticas de compartimentos de uso general de S3 deberían restringir el acceso a otros Cuentas de AWS](#)
- [\[S3.8\] Los buckets de uso general de S3 deben bloquear el acceso público](#)
- [\[S3.9\] Los buckets de uso general de S3 deben tener habilitado el registro de acceso al servidor](#)
- [\[S3.12\] no ACLs debe usarse para administrar el acceso de los usuarios a los depósitos de uso general de S3](#)
- [\[S3.13\] Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida](#)
- [\[S3.17\] Los depósitos de uso general de S3 deben cifrarse en reposo con AWS KMS keys](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] las instancias de SageMaker notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook](#)
- [\[SecretsManager.1\] Los secretos de Secrets Manager deberían tener habilitada la rotación automática](#)
- [\[SecretsManager.2\] Los secretos de Secrets Manager configurados con rotación automática deberían rotar correctamente](#)
- [\[SecretsManager.3\] Eliminar los secretos de Secrets Manager no utilizados](#)
- [\[SecretsManager.4\] Los secretos de Secrets Manager deben rotarse en un número específico de días](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SSM.1\] EC2 Las instancias de Amazon deben administrarse mediante AWS Systems Manager](#)

- [\[SSM.2\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de parche de COMPLIANT después de la instalación de un parche](#)
- [\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [\[SSM.4\] Los documentos SSM no deben ser públicos](#)
- [Las reglas de \[WAF.2\] Regionales AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.4\] Regionales AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [La AWS WAF web de \[WAF.10\] ACLs debe tener al menos una regla o grupo de reglas](#)

Para obtener más información sobre este estándar, consulte los [controles CSPM de Security Hub](#) en la Guía del AWS Control Tower usuario.

Habilitación de un estándar de seguridad

Al habilitar un estándar de seguridad en AWS Security Hub Cloud Security Posture Management (CSPM), Security Hub CSPM crea y habilita automáticamente todos los controles que se aplican al estándar. Security Hub CSPM también comienza a ejecutar controles de seguridad y a generar hallazgos para los controles.

Para optimizar la cobertura y la precisión de los hallazgos, habilite y configure el registro de recursos AWS Config antes de activar un estándar. Al configurar el registro de recursos, asegúrese también de habilitarlo para todos los tipos de recursos que se comprueban mediante los controles que se aplican al estándar. De lo contrario, es posible que Security Hub CSPM no pueda evaluar los recursos adecuados y generar resultados precisos para los controles que se aplican a la norma. Para obtener más información, consulte [Habilitación y configuración AWS Config de Security Hub CSPM](#).

Después de habilitar un estándar, puede deshabilitar o volver a habilitar más adelante los controles individuales que se apliquen al estándar. Si deshabilita un control para un estándar, Security Hub CSPM deja de generar hallazgos para el control. Además, Security Hub CSPM ignora el control cuando calcula la puntuación de seguridad del estándar. La puntuación de seguridad es el porcentaje de controles que han superado la evaluación, en relación con el número total de controles que se aplican al estándar, están activados y tienen datos de evaluación.

Al habilitar un estándar, Security Hub CSPM genera una puntuación de seguridad preliminar para el estándar, normalmente 30 minutos después de su primera visita a la página de resumen o

estándares de seguridad en la consola CSPM de Security Hub. Las puntuaciones de seguridad se generan únicamente para los estándares que están activados al visitar esas páginas de la consola. Además, el registro de recursos debe estar configurado AWS Config para que aparezcan las puntuaciones. En las regiones de China y AWS GovCloud (US) Regions, Security Hub CSPM puede tardar hasta 24 horas en generar una puntuación de seguridad preliminar para un estándar. Una vez que Security Hub CSPM genera una puntuación preliminar, la actualiza cada 24 horas. Para determinar cuándo se actualizó por última vez una puntuación de seguridad, puede consultar la marca de tiempo que Security Hub CSPM proporciona para la puntuación. Para obtener más información, consulte [Calcular las puntuaciones de seguridad](#).

La forma de habilitar un estándar depende de si utiliza la [configuración central](#) para administrar Security Hub (CSPM) para varias cuentas y. Regiones de AWS Recomendamos utilizar la configuración centralizada si desea habilitar los estándares en entornos con varias cuentas y regiones. Puede utilizar la configuración central si integra Security Hub CSPM con. AWS Organizations Si no utiliza la configuración central, debe habilitar cada estándar por separado en cada cuenta y región.

Temas

- [Habilitar un estándar en varias cuentas y Regiones de AWS](#)
- [Habilitar un estándar en una sola cuenta y Región de AWS](#)
- [Comprobar el estado de un estándar](#)

Habilitar un estándar en varias cuentas y Regiones de AWS

Para habilitar y configurar un estándar de seguridad en varias cuentas Regiones de AWS, utilice la [configuración central](#). Con la configuración central, el administrador de CSPM de Security Hub delegado puede crear políticas de configuración de CSPM de Security Hub que habiliten uno o más estándares. A continuación, el administrador puede asociar una política de configuración a cuentas individuales, unidades organizativas (OUs) o a la raíz. Una política de configuración afecta a la región de origen, también denominada región de agregación, y a todas las regiones vinculadas.

Las políticas de configuración ofrecen opciones de personalización. Por ejemplo, puede optar por habilitar solo el estándar de mejores prácticas de seguridad AWS fundamentales (FSBP) para una unidad organizativa. Para otra unidad organizativa, puede optar por habilitar tanto el estándar FSBP como el estándar Foundations Benchmark v1.4.0 del Center for Internet Security (CIS) AWS . Para obtener información sobre la creación de una política de configuración que habilite los estándares específicos que especifique, consulte. [Creación y asociación de políticas de configuración](#)

Si usa la configuración central, Security Hub CSPM no habilita automáticamente ningún estándar en las cuentas nuevas o existentes. En su lugar, el administrador de CSPM de Security Hub especifica qué estándares se deben habilitar en las diferentes cuentas cuando crea las políticas de configuración de CSPM de Security Hub para su organización. Security Hub CSPM ofrece una política de configuración recomendada en la que solo se habilita el estándar FSBP. Para obtener más información, consulte [Tipos de políticas de configuración](#).

 Note

El administrador CSPM de Security Hub puede usar políticas de configuración para habilitar cualquier estándar, excepto el estándar de administración de [AWS Control Tower servicios](#). Para habilitar este estándar, el administrador debe usarlo directamente. AWS Control Tower También deben utilizarse AWS Control Tower para activar o desactivar los controles individuales de este estándar para una cuenta gestionada de forma centralizada.

Si desea que algunas cuentas habiliten y configuren estándares para sus propias cuentas, el administrador CSPM de Security Hub puede designarlas como cuentas autogestionadas. Las cuentas autogestionadas deben habilitar y configurar los estándares por separado en cada región.

Habilitar un estándar en una sola cuenta y Región de AWS

Si no utiliza la configuración central o tiene una cuenta autogestionada, no podrá utilizar las políticas de configuración para habilitar de forma centralizada los estándares de seguridad en varias cuentas o Regiones de AWS. Sin embargo, puedes habilitar un estándar en una sola cuenta y región. Puede hacerlo mediante la consola CSPM de Security Hub o la API CSPM de Security Hub.

Security Hub CSPM console

Siga estos pasos para habilitar un estándar en una cuenta y región mediante la consola CSPM de Security Hub.

Habilitación de un estándar en una cuenta y región

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, elija la región en la que desee activar el estándar.

3. En el panel de navegación, elija Estándares de seguridad. La página de estándares de seguridad enumera todos los estándares que Security Hub CSPM admite actualmente. Si ya ha activado un estándar, la sección correspondiente al estándar incluye la puntuación de seguridad actual y detalles adicionales del estándar.
4. En la sección del estándar que desee habilitar, elija Habilitar estándar.

Para activar el estándar en otras regiones, repita los pasos anteriores en cada región adicional.

Security Hub CSPM API

Para habilitar un estándar mediante programación en una sola cuenta y región, utilice la [BatchEnableStandards](#) operación. O bien, si está utilizando AWS Command Line Interface (AWS CLI), ejecute el [batch-enable-standards](#) comando.

En su solicitud, utilice el `StandardsArn` parámetro para especificar el nombre de recurso de Amazon (ARN) del estándar que desee habilitar. Especifique también la región a la que se aplica la solicitud. Por ejemplo, el siguiente comando habilita el estándar AWS Foundational Security Best Practices (FSBP):

```
$ aws securityhub batch-enable-standards \
--standards-subscription-requests '{"StandardsArn":"arn:aws:securityhub:us-
east-1::standards/aws-foundational-security-best-practices/v/1.0.0"}' \
--region us-east-1
```

¿Dónde *arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0* está el ARN del estándar FSBP en la región EE.UU. Este (Virginia del Norte) y *us-east-1* es la región en la que se debe habilitar?

Para obtener el ARN de un estándar, utilice la [DescribeStandards](#) operación o, si utiliza el AWS CLI, ejecute el [describe-standards](#) comando.

Para revisar primero una lista de estándares que están actualmente habilitados en su cuenta, puede usar la [GetEnabledStandards](#) operación. Si utilizas el AWS CLI, puedes ejecutar el [get-enabled-standards](#) comando para recuperar esta lista.

Tras habilitar un estándar, Security Hub CSPM comienza a realizar tareas para habilitar el estándar en la cuenta y en la región especificada. Esto incluye la creación de todos los controles que se aplican al estándar. Para supervisar el estado de estas tareas, puede comprobar el estado de la norma para la cuenta y la región.

Comprobar el estado de un estándar

Al habilitar un estándar de seguridad para una cuenta, Security Hub CSPM comienza a crear todos los controles que se aplican al estándar en la cuenta. Security Hub CSPM también realiza tareas adicionales para habilitar el estándar para la cuenta, como generar una puntuación de seguridad preliminar para el estándar. Mientras Security Hub CSPM realiza estas tareas, el estado del estándar es el Pending de la cuenta. A continuación, el estado del estándar pasa por estados adicionales, que puede supervisar y comprobar.

Note

Los cambios en los controles individuales de una norma no afectan al estado general de la norma. Por ejemplo, si habilita un control que había desactivado anteriormente, el cambio no afectará al estado del estándar. Del mismo modo, si cambias el valor de un parámetro para un control activado, el cambio no afectará al estado del estándar.

Para comprobar el estado de un estándar mediante la consola CSPM de Security Hub, elija Estándares de seguridad en el panel de navegación. La página de estándares de seguridad enumera todos los estándares que Security Hub CSPM admite actualmente. Si Security Hub CSPM está realizando tareas para habilitar el estándar, la sección correspondiente al estándar indica que Security Hub CSPM sigue generando una puntuación de seguridad para el estándar. Si un estándar está activado, la sección correspondiente al estándar incluye la puntuación actual. Seleccione Ver resultados para revisar detalles adicionales, incluido el estado de los controles individuales que se aplican a la norma. Para obtener más información, consulte [Programación para ejecutar comprobaciones de seguridad](#).

Para comprobar el estado de un estándar mediante programación con la API CSPM de Security Hub, utilice la operación. [GetEnabledStandards](#) En su solicitud, si lo desea, utilice el StandardsSubscriptionArns parámetro para especificar el nombre de recurso de Amazon (ARN) del estándar cuyo estado desea comprobar. Si utiliza AWS Command Line Interface (AWS CLI), puede ejecutar el [get-enabled-standards](#) comando para comprobar el estado de un estándar. Para especificar el ARN del estándar que se va a comprobar, utilice el standards-subscription-arns parámetro. Para determinar qué ARN especificar, puede utilizar la [DescribeStandards](#) operación o, para ello AWS CLI, ejecutar el [describe-standards](#) comando.

Si la solicitud se realiza correctamente, Security Hub CSPM responde con una serie de objetos. StandardsSubscription Una suscripción estándar es un AWS recurso que Security Hub CSPM

crea en una cuenta cuando se habilita un estándar para la cuenta. Cada `StandardsSubscription` objeto proporciona detalles sobre un estándar que está actualmente activado o que se está activando o deshabilitando para la cuenta. Dentro de cada objeto, el `StandardsStatus` campo especifica el estado actual del estándar de la cuenta.

El estado de un estándar (`StandardsStatus`) puede ser uno de los siguientes.

PENDING

Security Hub (CSPM) está realizando tareas para habilitar el estándar para la cuenta. Esto incluye la creación de los controles que se aplican al estándar y la generación de una puntuación de seguridad preliminar para el estándar. Security Hub CSPM puede tardar varios minutos en completar todas las tareas. Un estándar también puede tener este estado si ya está activado para la cuenta y Security Hub CSPM está añadiendo nuevos controles al estándar.

Si un estándar tiene este estado, es posible que no puedas recuperar los detalles de los controles individuales que se aplican al estándar. Además, es posible que no pueda configurar o deshabilitar los controles individuales del estándar. Por ejemplo, si intenta deshabilitar un control mediante la [UpdateStandardsControl](#) operación, se produce un error.

Para determinar si puede configurar o administrar de otro modo los controles individuales para el estándar, consulte el valor del `StandardsControlsUpdatable` campo. Si el valor de este campo es `READY_FOR_UPDATES`, puede empezar a gestionar los controles individuales del estándar. De lo contrario, espere a que Security Hub CSPM complete las tareas de procesamiento adicionales para habilitar el estándar.

READY

El estándar está activado actualmente para la cuenta. Security Hub CSPM puede ejecutar comprobaciones de seguridad y generar resultados para todos los controles que se aplican al estándar y que están habilitados actualmente. Security Hub CSPM también puede calcular una puntuación de seguridad para el estándar.

Si una norma tiene este estado, puede recuperar los detalles de los controles individuales que se aplican a la norma. Además, puede configurar, deshabilitar o volver a activar los controles. También puede desactivar el estándar.

INCOMPLETE

Security Hub CSPM no pudo habilitar el estándar por completo para la cuenta. Security Hub CSPM no puede ejecutar comprobaciones de seguridad ni generar resultados para todos los

controles que se aplican al estándar y que están habilitados actualmente. Además, Security Hub CSPM no puede calcular una puntuación de seguridad para el estándar.

Para determinar por qué el estándar no se habilitó por completo, consulte la información de la `StandardsStatusReason` matriz. Esta matriz especifica los problemas que impidieron que Security Hub CSPM habilitara el estándar. Si se ha producido un error interno, intente volver a activar el estándar para la cuenta. Para otros tipos de problemas, [comprueba AWS Config la configuración](#). También puedes [desactivar los controles individuales](#) que no quieras comprobar o desactivar el estándar por completo.

DELETING

Security Hub CSPM está procesando actualmente una solicitud para deshabilitar el estándar de la cuenta. Esto incluye deshabilitar los controles que se aplican al estándar y eliminar la puntuación de seguridad asociada. El Security Hub CSPM puede tardar varios minutos en terminar de procesar la solicitud.

Si un estándar tiene este estado, no puede volver a activarlo ni intentar deshabilitarlo de nuevo para la cuenta. Security Hub CSPM debe terminar de procesar primero la solicitud actual. Además, no puede recuperar los detalles de los controles individuales que se aplican al estándar ni administrar los controles.

FAILED

Security Hub CSPM no ha podido inhabilitar el estándar para la cuenta. Se produjeron uno o más errores cuando el Security Hub CSPM intentó deshabilitar el estándar. Además, Security Hub CSPM no puede calcular una puntuación de seguridad para el estándar.

Para determinar por qué el estándar no se deshabilitó por completo, consulte la información de la `StandardsStatusReason` matriz. Esta matriz especifica los problemas que impidieron que Security Hub CSPM deshabilitara el estándar.

Si un estándar tiene este estado, no podrá recuperar los detalles de los controles individuales que se aplican al estándar ni administrar los controles. Sin embargo, puedes volver a activar el estándar para la cuenta. Si soluciona los problemas que impidieron que Security Hub CSPM deshabilitara el estándar, también puede intentar deshabilitarlo nuevamente.

Si el estado de un estándar es `READY`, Security Hub CSPM ejecuta comprobaciones de seguridad y genera resultados para todos los controles que se aplican al estándar y que están habilitados actualmente. Para otros estados, el CSPM de Security Hub puede ejecutar comprobaciones y

generar resultados para algunos controles habilitados, pero no para todos. Generar o actualizar los resultados de los controles puede tardar hasta 24 horas. Para obtener más información, consulte [Programación para ejecutar comprobaciones de seguridad](#).

Revisar los detalles de un estándar de seguridad

Después de habilitar un estándar de AWS seguridad en Security Hub Cloud Security Posture Management (CSPM), puede usar la consola para revisar los detalles del estándar. En la consola de , la página de detalles de un estándar incluye la siguiente información:

- La puntuación de seguridad actual del estándar.
- Una tabla de controles que se aplican al estándar.
- Estadísticas agregadas de los controles que se aplican a la norma.
- Un resumen visual del estado de los controles que se aplican a la norma.
- Un resumen visual de las comprobaciones de seguridad de los controles que están habilitados y se aplican a la norma. Si se integra con AWS Organizations, los controles que estén habilitados en al menos una cuenta de la organización se considerarán habilitados.

Para revisar estos detalles, elija Normas de seguridad en el panel de navegación de la consola. A continuación, en la sección correspondiente a la norma, selecciona Ver resultados. Para un análisis más profundo, puede filtrar y ordenar los datos y profundizar para revisar los detalles de los controles individuales que se aplican a la norma.

Temas

- [Descripción de la puntuación de seguridad del estándar](#)
- [Revisar los controles para determinar si existe una norma](#)

Descripción de la puntuación de seguridad del estándar

En la consola AWS Security Hub Cloud Security Posture Management (CSPM), la página de detalles de un estándar muestra la puntuación de seguridad del estándar. La puntuación es el porcentaje de controles que han superado la evaluación, en relación con el número total de controles que se aplican al estándar, están activados y tienen datos de evaluación. Debajo de la puntuación hay un gráfico que resume las comprobaciones de seguridad de los controles que están habilitados para el estándar. Esto incluye el número de controles de seguridad aprobados y no aprobados.

En el caso de las cuentas de administrador, la puntuación y el gráfico estándar se agregan en la cuenta de administrador y en todas las cuentas de los miembros. Para revisar las comprobaciones de seguridad no aprobadas para ver si los controles tienen una gravedad específica, seleccione la gravedad.

Cuando habilita un estándar, Security Hub CSPM genera una puntuación de seguridad preliminar para el estándar, normalmente 30 minutos después de su primera visita a la página de resumen o a la página de estándares de seguridad de la consola CSPM de Security Hub. Las puntuaciones se generan únicamente para los estándares que están activados al visitar esas páginas. Además, se debe configurar el registro de AWS Config recursos para que aparezcan las partituras. En las regiones de China y AWS GovCloud (US) Regions, Security Hub CSPM puede tardar hasta 24 horas en generar una puntuación preliminar. Una vez que Security Hub CSPM genera una puntuación preliminar para un estándar, la actualiza cada 24 horas. Para obtener más información, consulte [Calcular las puntuaciones de seguridad](#).

Todos los datos de las páginas de detalles de las normas de seguridad son específicos de las actuales, a Región de AWS menos que establezca una región de agregación. Si estableces una región de agregación, los puntajes de seguridad se aplican a todas las regiones e incluyen los resultados de todas las regiones vinculadas. Además, el estado de cumplimiento de los controles refleja los hallazgos de las regiones vinculadas, y el número de controles de seguridad incluye los hallazgos de las regiones vinculadas.

Revisar los controles para determinar si existe una norma

Cuando utilizas la consola de AWS Security Hub Cloud Security Posture Management (CSPM) para revisar los detalles de un estándar que has activado, puedes revisar una tabla de controles de seguridad que se aplican al estándar. Para cada control, la tabla incluye la siguiente información:

- El identificador y el título del control.
- El estado del control. Para obtener más información, consulte [Evaluación del estado de cumplimiento y el estado de control](#).
- La gravedad asignada al control.
- El número de comprobaciones fallidas y el número total de comprobaciones. Si corresponde, el campo Comprobaciones fallidas también especifica el número de hallazgos con el estado Desconocido.
- Si el control admite parámetros personalizados. Para obtener más información, consulte [Descripción de los parámetros de control en Security Hub CSPM](#).

Security Hub CSPM actualiza los estados de control y el recuento de las comprobaciones de seguridad cada 24 horas. Una marca de tiempo en la parte superior de la página indica cuándo Security Hub CSPM actualizó estos datos por última vez.

En el caso de las cuentas de administrador, los estados de control y el número de comprobaciones de seguridad se agregan a la cuenta de administrador y a todas las cuentas de los miembros. El recuento de controles habilitados incluye los controles que están habilitados para el estándar en la cuenta de administrador o al menos en la cuenta de un miembro. El recuento de controles deshabilitados incluye los controles que están deshabilitados de forma estándar en la cuenta de administrador y en todas las cuentas de los miembros.

Puede filtrar la tabla de controles que se aplica a la norma. Con las opciones Filtrar por que aparecen junto a la tabla, puede elegir ver solo los controles activados o desactivados de la norma. Si solo muestra los controles activados, puede filtrar aún más la tabla por estado de control. A continuación, puede centrarse en los controles que tienen un estado de control específico. Además de las opciones Filtrar por, puede introducir los criterios de filtrado en el cuadro de controles de filtrado. Por ejemplo, puede filtrar por ID o título de control.

Elija el método de acceso que prefiera. A continuación, siga los pasos para revisar los controles que se aplican a un estándar que haya activado.

Security Hub CSPM console

Para revisar los controles de un estándar habilitado

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
2. Elija Estándares de seguridad en el panel de navegación.
3. En la sección del estándar, selecciona Ver resultados.

La tabla de la parte inferior de la página muestra todos los controles que se aplican a la norma. Puede filtrar y ordenar la tabla. También puede descargar la página actual de la tabla como un archivo CSV. Para ello, selecciona Descargar encima de la tabla. Si filtra la tabla, el archivo descargado incluye solo los controles que coinciden con la configuración de filtro actual.

Security Hub CSPM API

Para revisar los controles de un estándar habilitado

1. Utilice el [ListSecurityControlDefinitions](#) funcionamiento de la API CSPM de Security Hub. Si está utilizando el AWS CLI, ejecute el [list-security-control-definitions](#) comando.

Especifique el nombre de recurso de Amazon (ARN) del estándar cuyos controles desee revisar. ARNs Para obtener los estándares, utilice la [DescribeStandards](#) operación o ejecute el comando [describe-standards](#). Si no especifica el ARN de un estándar, el CSPM de Security Hub devuelve todo el control de seguridad. IDs

2. Utilice la [ListStandardsControlAssociations](#) operación de la API CSPM de Security Hub o ejecute el [list-standards-control-associations](#) comando. Esta operación indica en qué estándares está activado un control.

Identifique el control proporcionando el ARN o ID del control de seguridad. Los parámetros de paginación son opcionales.

El siguiente ejemplo indica en qué estándares está habilitado el control Config. 1.

```
$ aws securityhub list-standards-control-associations --region us-east-1 --security-control-id Config.1
```

Desactivar los estándares de seguridad activados automáticamente

Si su organización no utiliza la configuración central, utiliza un tipo de configuración denominado configuración local. Con la configuración local, AWS Security Hub Cloud Security Posture Management (CSPM) puede habilitar automáticamente los estándares de seguridad predeterminados para las cuentas de los nuevos miembros cuando las cuentas se unan a su organización. Todos los controles que se aplican a estos estándares predeterminados también se activan automáticamente.

Actualmente, los estándares de seguridad predeterminados son el estándar AWS Foundational Security Best Practices y el estándar AWS Foundations Benchmark v1.2.0 del Center for Internet Security (CIS). Para obtener información sobre estos estándares, consulte la [Referencia de estándares para Security Hub CSPM](#)

Si prefiere activar manualmente los estándares de seguridad para las cuentas de los nuevos miembros, puede desactivar la activación automática de los estándares predeterminados. Solo puede hacerlo si se integra con la configuración local AWS Organizations y la utiliza. Si utiliza la configuración central, puede crear una política de configuración que habilite los estándares predeterminados y asocie la política a la raíz. Todas las cuentas de la organización y OUs, a continuación, heredar esta política de configuración, a menos que estén asociadas a una política diferente o se administren automáticamente. Si no se integra con AWS Organizations, puede deshabilitar un estándar predeterminado al habilitar inicialmente el Security Hub CSPM o una versión posterior. Para aprender a hacerlo, consulte [Desactivación de un estándar](#).

Para desactivar la activación automática de los estándares predeterminados para las cuentas de los nuevos miembros, puede utilizar la consola CSPM de Security Hub o la API CSPM de Security Hub.

Security Hub CSPM console

Siga estos pasos para desactivar la activación automática de los estándares predeterminados mediante la consola CSPM de Security Hub.

Para desactivar la activación automática de los estándares predeterminados

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>.
Inicie sesión en las credenciales de una cuenta del administrador.
2. En el panel de navegación, en Configuración, elija Configuración.
3. En la sección Información general, seleccione Editar.
4. En Configuración de la nueva cuenta, desactive la casilla Habilitar los estándares de seguridad predeterminados.
5. Elija Confirmar.

Security Hub CSPM API

Para desactivar la activación automática de los estándares predeterminados mediante programación, desde la cuenta de administrador CSPM de Security Hub, utilice la operación de [UpdateOrganizationConfiguration](#) la API CSPM de Security Hub. En su solicitud, especifique el parámetro. `NONE AutoEnableStandards`

Si está utilizando el AWS CLI, ejecute el [update-organization-configuration](#) comando para desactivar la activación automática de los estándares predeterminados. En el parámetro

`auto-enable-standards`, especifique `NONE`. Por ejemplo, el siguiente comando habilita automáticamente el CSPM de Security Hub para las cuentas de los nuevos miembros y desactiva la activación automática de los estándares predeterminados para las cuentas.

```
$ aws securityhub update-organization-configuration --auto-enable --auto-enable-standards NONE
```

Deshabilitación de un estándar de seguridad

Al deshabilitar un estándar de seguridad en AWS Security Hub Cloud Security Posture Management (CSPM), ocurre lo siguiente:

- Todos los controles que se aplican al estándar están deshabilitados, a menos que estén asociados a otro estándar que esté activado actualmente.
- Ya no se realizan controles de seguridad para los controles desactivados y no se generan más resultados en relación con los controles desactivados.
- Los hallazgos existentes sobre los controles desactivados se archivan automáticamente después de aproximadamente 3 a 5 días.
- AWS Config se eliminan las reglas que Security Hub CSPM creó para los controles deshabilitados.

Por lo general, la eliminación de AWS Config las reglas correspondientes se produce a los pocos minutos de haber desactivado un estándar. Sin embargo, es posible que tarde más. Si la primera solicitud no elimina las reglas, Security Hub CSPM vuelve a intentarlo cada 12 horas. Sin embargo, si has desactivado Security Hub CSPM o no has activado ningún otro estándar, Security Hub CSPM no podrá volver a intentarlo, lo que significa que no podrá eliminar las reglas. Si esto ocurre y necesita eliminar las reglas, póngase en contacto con nosotros. AWS Support

Temas

- [Deshabilitar un estándar en varias cuentas y Regiones de AWS](#)
- [Deshabilitar un estándar en una sola cuenta y Región de AWS](#)

Deshabilitar un estándar en varias cuentas y Regiones de AWS

Para deshabilitar un estándar de seguridad en varias cuentas Regiones de AWS, utilice la [configuración central](#). Con la configuración central, el administrador de CSPM de Security Hub

delegado puede crear políticas de configuración de CSPM de Security Hub que inhabiliten uno o más estándares. A continuación, el administrador puede asociar una política de configuración a cuentas individuales, unidades organizativas (OUs) o a la raíz. Una política de configuración afecta a la región de origen, también denominada región de agregación, y a todas las regiones vinculadas.

Las políticas de configuración ofrecen opciones de personalización. Por ejemplo, puede optar por deshabilitar el Estándar de seguridad de datos del sector de las tarjetas de pago (PCI DSS) en una unidad organizativa. En el caso de otra unidad organizativa, puede optar por deshabilitar tanto el PCI DSS como el estándar SP 800-53 rev. 5 del Instituto Nacional de Estándares y Tecnología (NIST). Para obtener información sobre cómo crear una política de configuración que habilite o deshabilite los estándares individuales que especifique, consulte. [Creación y asociación de políticas de configuración](#)

Note

El administrador CSPM de Security Hub puede usar políticas de configuración para deshabilitar cualquier estándar, excepto el estándar de administración de [AWS Control Tower servicios](#). Para deshabilitar este estándar, el administrador debe usarlo directamente. AWS Control Tower También se deben usar AWS Control Tower para deshabilitar o habilitar los controles individuales de este estándar para una cuenta administrada de forma centralizada.

Si desea que algunas cuentas configuren o deshabiliten los estándares para sus propias cuentas, el administrador CSPM de Security Hub puede designarlas como cuentas autogestionadas. Las cuentas autogestionadas deben deshabilitar los estándares por separado en cada región.

Deshabilitar un estándar en una sola cuenta y Región de AWS

Si no utiliza la configuración central o tiene una cuenta autogestionada, no podrá utilizar las políticas de configuración para deshabilitar de forma centralizada los estándares de seguridad en varias cuentas o. Regiones de AWS Sin embargo, puedes deshabilitar un estándar en una sola cuenta y región. Puede hacerlo mediante la consola CSPM de Security Hub o la API CSPM de Security Hub.

Security Hub CSPM console

Siga estos pasos para deshabilitar un estándar en una cuenta y región mediante la consola CSPM de Security Hub.

Deshabilitación de un estándar en una cuenta y región

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, elija la región en la que desee desactivar el estándar.
3. En el panel de navegación, elija Estándares de seguridad.
4. En la sección del estándar que desee deshabilitar, elija Desactivar estándar.

Para deshabilitar el estándar en otras regiones, repita los pasos anteriores en cada región adicional.

Security Hub CSPM API

Para deshabilitar un estándar mediante programación en una sola cuenta y región, utilice la [BatchDisableStandards](#) operación. O bien, si usas AWS Command Line Interface (AWS CLI), ejecuta el [batch-disable-standards](#) comando.

En su solicitud, utilice el `StandardsSubscriptionArns` parámetro para especificar el nombre de recurso de Amazon (ARN) del estándar que desee deshabilitar. Si utiliza el AWS CLI, utilice el `standards-subscription-arns` parámetro para especificar el ARN. Especifique también la región a la que se aplica la solicitud. Por ejemplo, el siguiente comando desactiva el estándar de mejores prácticas de seguridad AWS fundamentales (FSBP) para una cuenta (): **123456789012**

```
$ aws securityhub batch-disable-standards \
--standards-subscription-arns "arn:aws:securityhub:us-
east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0" \
--region us-east-1
```

¿Dónde **arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0** está el ARN del estándar FSBP para la cuenta en la región EE.UU. Este (Virginia del Norte) y **us-east-1** es la región en la que se debe deshabilitar?

Para obtener el ARN de un estándar, puede utilizar la [GetEnabledStandards](#) operación. Esta operación recupera información sobre los estándares que están actualmente habilitados en su cuenta. Si utilizas el AWS CLI, puedes ejecutar el [get-enabled-standards](#) comando para recuperar esta información.

Tras deshabilitar un estándar, Security Hub CSPM comienza a realizar tareas para inhabilitar el estándar en la cuenta y en la región especificada. Esto incluye deshabilitar todos los controles que se aplican al estándar. Para supervisar el estado de estas tareas, puedes [comprobar el estado de la norma para la](#) cuenta y la región.

Descripción de los controles de seguridad en Security Hub CSPM

En AWS Security Hub Cloud Security Posture Management (CSPM), un control de seguridad, también denominado control, es una salvaguardia dentro de un estándar de seguridad que ayuda a una organización a proteger la confidencialidad, integridad y disponibilidad de su información. En Security Hub CSPM, un control está relacionado con un recurso específico AWS .

Cuando habilita un control en uno o más estándares, Security Hub CSPM comienza a ejecutar comprobaciones de seguridad en él. Las comprobaciones de seguridad dan como resultado las conclusiones del CSPM de Security Hub. Al deshabilitar un control, Security Hub CSPM deja de ejecutar las comprobaciones de seguridad en él y dejan de generarse los resultados.

Puede activar o desactivar los controles de forma individual para una sola cuenta y. Región de AWS Para ahorrar tiempo y reducir los errores de configuración en los entornos multicuenta, recomendamos utilizar la [configuración centralizada](#) para activar o desactivar los controles. Con la configuración central, el administrador de CSPM de Security Hub delegado puede crear políticas que especifiquen cómo debe configurarse un control en varias cuentas y regiones. Para obtener más información sobre cómo habilitar y deshabilitar controles, consulte [Habilitación de controles en Security Hub \(CSPM\)](#).

Vista de controles consolidados

La página de controles de la consola CSPM de Security Hub muestra todos los controles disponibles en la versión actual Región de AWS (puede ver los controles en el contexto de un estándar visitando la página de estándares de seguridad y seleccionando un estándar activado). Security Hub CSPM asigna a los controles un identificador, un título y una descripción de control de seguridad coherentes en todos los estándares. IDs Los controles incluyen el número correspondiente Servicio de AWS y un número único (por ejemplo, CodeBuild .3).

La siguiente información está disponible en la página de controles de la consola [CSPM de Security Hub](#):

- Una puntuación general de seguridad basada en la proporción de controles aprobados en comparación con el número total de controles habilitados con datos
- Desglose de los estados de control en todos los controles CSPM de Security Hub compatibles
- El número total de controles de seguridad aprobados y con fallos.

- El número de controles de seguridad con fallos para controles de diferente gravedad y los enlaces para ver más detalles sobre esos controles de seguridad con fallos.
- Una lista de controles CSPM de Security Hub, con filtros para ver subconjuntos específicos de controles.

En la página Controles, puede elegir un control para ver sus detalles y tomar medidas en función de los resultados generados por el control. Desde esta página, también puede activar o desactivar un control de seguridad en su actual y. Cuenta de AWS Región de AWS Las acciones de activación y desactivación de la página Controles se aplican a todos los estándares. Para obtener más información, consulte [Habilitación de controles en Security Hub \(CSPM\)](#).

En el caso de las cuentas de administrador, la página Controles refleja el estado de los controles en las cuentas de los miembros. Si se produce un error en una comprobación de control en al menos una cuenta miembro, el estado de control es Con error. Si ha establecido una [región de agregación](#), la página Controles refleja el estado de los controles en todas las regiones vinculadas. Si se produce un error en una comprobación de control en al menos una región vinculada, el estado del control es Con error.

La vista de controles consolidados provoca cambios en los campos de búsqueda de controles en el formato AWS de búsqueda de seguridad (ASFF) que pueden afectar a los flujos de trabajo. Para obtener más información, consulte [Vista de controles consolidada: cambios en ASFF](#).

Puntuación general de seguridad de los controles

La página Controles muestra una puntuación de seguridad general que va del 0 al 100 por ciento. La puntuación de seguridad general se calcula en función de la proporción de controles aprobados en comparación con el número total de controles habilitados con datos en todos los estándares.

Note

Para ver la puntuación de seguridad general de los controles, debe añadir permiso de llamada **BatchGetControlEvaluations** al rol de IAM que utiliza para acceder a Security Hub CSPM. Este permiso no es necesario para ver las puntuaciones de seguridad según estándares específicos.

Al activar Security Hub CSPM, Security Hub CSPM calcula la puntuación de seguridad inicial 30 minutos después de su primera visita a la página de resumen o a la página de normas de seguridad

de la consola CSPM de Security Hub. Las puntuaciones de seguridad por primera vez pueden tardar hasta 24 horas en generarse en las regiones de China y de AWS GovCloud (US) Regions.

Además de la puntuación de seguridad general, Security Hub CSPM calcula una puntuación de seguridad estándar para cada estándar habilitado 30 minutos después de su primera visita a la página de resumen o a la página de normas de seguridad. Para ver una lista de los estándares que están habilitados actualmente, utilice la operación de API [GetEnabledStandards](#).

AWS Config debe estar habilitado con el registro de recursos para que aparezcan las partituras. Para obtener información sobre cómo Security Hub CSPM calcula las puntuaciones de seguridad, consulte. [Calcular las puntuaciones de seguridad](#)

Tras la primera generación de puntuaciones, Security Hub CSPM actualiza las puntuaciones de seguridad cada 24 horas. Security Hub CSPM muestra una marca de tiempo para indicar cuándo se actualizó por última vez una puntuación de seguridad.

Si ha establecido una región de agregación, la puntuación de seguridad general refleja los resultados de control en las regiones vinculadas.

Referencia de control para Security Hub CSPM

Esta referencia de control proporciona una lista de los controles de AWS Security Hub Cloud Security Posture Management (CSPM) disponibles con enlaces a más información sobre cada control. La tabla de información general muestra los controles en orden alfabético por identificador de control. Aquí solo se incluyen los controles que Security Hub CSPM utiliza activamente. Los controles retirados se excluyen de esta lista. La tabla proporciona la siguiente información para cada control:

- ID de control de seguridad: este ID se aplica a todos los estándares e indica el Servicio de AWS recurso al que se refiere el control. La consola CSPM de Security Hub muestra el control de seguridad IDs, independientemente de si los [hallazgos de control consolidados](#) están activados o desactivados en su cuenta. Sin embargo, las conclusiones del CSPM de Security Hub IDs solo hacen referencia al control de seguridad si las conclusiones del control consolidado están activadas en su cuenta. Si las conclusiones de control consolidadas están desactivadas en su cuenta, algunos controles IDs varían según el estándar en sus conclusiones de control. Para ver un mapeo entre el control específico de un estándar y el control IDs de seguridad IDs, consulte. [Cómo afecta la consolidación al control IDs y a los títulos](#)

Si desea configurar las [automatizaciones](#) de los controles de seguridad, le recomendamos que filtre en función del identificador del control y no del título o la descripción. Mientras que Security

Hub CSPM puede actualizar ocasionalmente los títulos o descripciones de los controles, el control sigue IDs siendo el mismo.

El control IDs puede omitir números. Estos son marcadores de posición para futuros controles.

- Normas aplicables: indica a qué normas se aplica un control. Elija un control para revisar los requisitos específicos de los marcos de cumplimiento de terceros.
- Título de control de seguridad: este título se aplica a todos los estándares. La consola CSPM de Security Hub muestra los títulos de los controles de seguridad, independientemente de si los hallazgos de control consolidados están activados o desactivados en su cuenta. Sin embargo, las conclusiones de CSPM de Security Hub hacen referencia a los títulos de control de seguridad solo si las conclusiones de control consolidadas están activadas en su cuenta. Si los resultados de control consolidados están desactivados en su cuenta, algunos títulos de control varían según el estándar en los resultados de control. Para ver un mapeo entre el control específico de un estándar y el control de seguridad IDs, consulte. IDs [Cómo afecta la consolidación al control IDs y a los títulos](#)
- Gravedad: la gravedad de un control identifica su importancia desde el punto de vista de la seguridad. Para obtener información sobre cómo el CSPM de Security Hub determina la gravedad del control, consulte. [Niveles de gravedad de los hallazgos de control](#)
- Tipo de programa: indica cuándo se evalúa el control. Para obtener más información, consulte [Programación para ejecutar comprobaciones de seguridad](#).
- Admite parámetros personalizados: indica si el control admite valores personalizados para uno o varios parámetros. Elija un control para revisar los detalles de los parámetros. Para obtener más información, consulte [Descripción de los parámetros de control en Security Hub CSPM](#).

Elija un control para revisar los detalles adicionales. Los controles se muestran en orden alfabético por identificador de control de seguridad.

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Account.1	La información de contacto de seguridad debe proporcionarse para un Cuenta de AWS	CIS AWS Foundations Benchmark v3.0.0, AWS Foundational Security Best Practices v1.0.0, estándar de gestión de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Periódico
Account.2	Cuenta de AWS debe ser parte de una organización	NIST SP 800-53 Rev. 5	ALTO	 No	Periódico
ACM.1	Los certificados importados y emitidos por ACM deben renovarse después de un período de tiempo específico	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 rev. 5 AWS Control Tower, NIST SP 800-171 rev. 2, PCI DSS v4.0.1	MEDIO	 Sí	El cambio se desencadena y es periódico
ACM.2	Los certificados RSA administrados por ACM deben usar una longitud de clave de al menos 2048 bits	AWS Mejores prácticas fundamentales de seguridad v1.0.0, PCI DSS v4.0.1	ALTO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ACM.3	Los certificados ACM deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Amplify r.1	Amplify: las aplicaciones deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Amplify r.2	Amplify branches debe estar etiquetado	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
APIGateway1.	El registro de ejecución de WebSocket API Gateway REST y API debe estar habilitado	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 rev. AWS Control Tower 5	MEDIO	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
APIGateway2.	Las etapas de la API de REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 rev. 5 AWS Control Tower, NIST SP 800-171 rev. 2	MEDIO	 No	El cambio se ha activado
APIGateway3.	Las etapas de la API REST de API Gateway deberían tener AWS X-Ray el rastreo habilitado	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 rev. 5	BAJA	 No	El cambio se ha activado
APIGateway4.	La API de Gateway debe estar asociada a una ACL web de WAF	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
APIGateway5.	Los datos de la caché de la API de REST de API Gateway deben cifrarse en reposo	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
APIGateway8.	Las rutas de API Gateway deben especificar un tipo de autorización	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	MEDIO	 Sí	Periódico
APIGateway9.	El registro de acceso debe configurarse para las etapas V2 de API Gateway	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 rev. 5 AWS Control Tower, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
AppConfig 1.	AWS AppConfig las aplicaciones deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
AppConfig 2.	AWS AppConfig los perfiles de configuración deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
AppConfig 3.	AWS AppConfig los entornos deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
AppConfig 4.	AWS AppConfig las asociaciones de extensiones deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
AppFlow 1.	AppFlow Los flujos de Amazon deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
AppRunner 1.	Los servicios de App Runner deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
AppRunner2.	Los conectores VPC de App Runner deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
AppSync1.	AWS AppSync Las cachés de las API deben estar cifradas en reposo	AWS Mejores prácticas de seguridad fundamentales	MEDIO	 No	El cambio se ha activado
AppSync2.	AWS AppSync debe tener habilitado el registro a nivel de campo	AWS Mejores prácticas fundamentales de seguridad v1.0.0, PCI DSS v4.0.1	MEDIO	 Sí	El cambio se ha activado
AppSync4.	AWS AppSync GraphQL APIs debe estar etiquetado	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
AppSync5.	AWS AppSync GraphQL no APIs debe autenticarse con claves de API	AWS Mejores prácticas fundamentales de seguridad, versión 1.0.0, NIST SP 800-53 Rev. 5	ALTO	 No	El cambio se ha activado
AppSync6.	AWS AppSync Las cachés de las API deben cifrarse en tránsito	AWS Mejores prácticas de seguridad fundamentales	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Athena.2	Los catálogos de datos de Athena deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Athena.3	Los grupos de trabajo de Athena deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Athena.4	Los grupos de trabajo de Athena deben tener el registro habilitado	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 No	El cambio se ha activado
AutoScaling1.	Los grupos de escalado automático o asociados con un equilibrador de carga deben usar comprobaciones de estado de ELB	AWS Mejores prácticas fundamentales de seguridad, estándar de gestión de servicios: PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	BAJA	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
AutoScaling2.	El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	MEDIO	 Sí	El cambio se ha activado
AutoScaling3.	Las configuraciones de lanzamiento de grupos de Auto Scaling deberían configurar EC2 las instancias para que requieran la versión 2 del servicio de metadatos de instancias (IMDSv2)	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower, PCI DSS v4.0.1	ALTO	 No	El cambio se ha activado
AutoScaling5.	EC2 Las instancias de Amazon lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower, PCI DSS v4.0.1	ALTO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
AutoScaling6.	Los grupos de escalado automático o deben usar varios tipos de instancias en varias zonas de disponibilidad	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
AutoScaling9.	EC2 Los grupos de Auto Scaling deben usar plantillas de EC2 lanzamiento	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	MEDIO	 No	El cambio se ha activado
AutoScaling1.10	EC2 Los grupos de Auto Scaling deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Backup.1	AWS Backup Los puntos de recuperación deben estar cifrados en reposo	AWS Prácticas recomendadas fundamentales de seguridad, versión 1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Backup.2	AWS Backup los puntos de recuperación deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Backup.3	AWS Backup Las bóvedas deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Backup.4	AWS Backup los planes de informes deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Backup.5	AWS Backup los planes de respaldo deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Lote.1	Las colas de trabajos por lotes deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Lote.2	Las políticas de programación de lotes deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Lote 3	Los entornos de procesamiento por lotes deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Lote 4	Las propiedades de los recursos informáticos en los entornos de procesamiento por lotes gestionados deben etiquetarse	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
CloudFormation2.	CloudFormation las pilas deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
CloudFront1.	CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	 No	El cambio se ha activado
CloudFront3.	CloudFront las distribuciones deberían requerir el cifrado en tránsito	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudFront t4.	CloudFront las distribuciones deben tener configurada la conmutación por error de origen	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 Rev. 5	BAJA	 No	El cambio se ha activado
CloudFront t5.	CloudFront las distribuciones deberían tener el registro habilitado	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
CloudFront t6.	CloudFront las distribuciones deben tener WAF habilitado	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
CloudFront t7.	CloudFront las distribuciones deben usar certificados personalizados SSL/TLS	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudFront t8.	CloudFront las distribuciones deben usar el SNI para atender las solicitudes HTTPS	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 Rev. 5	BAJA	 No	El cambio se ha activado
CloudFront t9.	CloudFront las distribuciones deben cifrar el tráfico hacia orígenes personalizados	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, NIST SP 800-53 rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
CloudFront t1.10	CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones de borde y los orígenes personalizados	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
CloudFront t1.2	CloudFront las distribuciones no deben apuntar a orígenes S3 inexistentes	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, NIST SP 800-53 rev. 5, PCI DSS v4.0.1	ALTO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudFront t1.3	CloudFront las distribuciones deben usar el control de acceso al origen	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO	 No	El cambio se ha activado
CloudFront t1.4	CloudFront las distribuciones deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
CloudTrail t1.	CloudTrail debe habilitarse y configurarse con al menos un registro multirregional que incluya eventos de administración de lectura y escritura	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, prácticas recomendadas de seguridad AWS fundamentales, estándar de gestión de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	ALTO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudTrail I2.	CloudTrail debe tener habilitada la encriptación en reposo	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0 AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, estándar de gestión de servicios: AWS Control Tower	MEDIO	 No	Periódico
CloudTrail I3.	Debe estar habilitado al menos un CloudTrail sendero	NIST SP 800-171 rev. 2, PCI DSS v4.0.1, PCI DSS v3.2.1	ALTO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudTrail I4.	CloudTrail La validación del archivo de registro debe estar habilitada	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, PCI DSS v3.2.1, estándar de gestión de servicios: AWS Control Tower	BAJA	 No	Periódico
CloudTrail I5.	CloudTrail los senderos deben estar integrados con Amazon CloudWatch Logs	CIS AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	BAJA	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudTrail I6.	Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público	CIS AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, PCI DSS v4.0.1	CRÍTICO	 No	El cambio se desencadena y es periódico
CloudTrail I7.	Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3	CIS AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v3.0.0, PCI AWS DSS v4.0.1	BAJA	 No	Periódico
CloudTrail I9.	CloudTrail los senderos deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
CloudTrail I.10	CloudTrail Los almacenes de datos de eventos de Lake deben estar cifrados y gestionados por el cliente AWS KMS keys	NIST SP 800-53 Rev. 5	MEDIO	 Sí	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudWatch h1.	Debe existir un filtro de métrica de registro y una alarma para el uso del usuario raíz	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2, PCI DSS v3.2.1	BAJA	 No	Periódico
CloudWatch h2.	Asegurar que haya un filtro de métricas de registro y alarma para las llamadas a la API no autorizadas	Índice de referencia CIS AWS Foundations v1.2.0, NIST SP 800-171 rev. 2	BAJA	 No	Periódico
CloudWatch h3.	Garantizar que haya un filtro de métricas de registro y una alarma de registro para el inicio de sesión en la sin MFA en la consola de administración	Punto de referencia sobre AWS los fundamentos de la CEI v1.2.0	BAJA	 No	Periódico
CloudWatch h4.	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios de política de IAM	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2	BAJA	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudWatch h5.	Asegúrese de que existan un registro métrico, un filtro y una alarma para los cambios CloudTrail de configuración	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2	BAJA	 No	Periódico
CloudWatch h6.	Asegúrese de que existan un filtro de métricas de registro y una alarma para detectar errores de AWS Management Console autenticación	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2	BAJA	 No	Periódico
CloudWatch h7.	Asegúrese de que existan un registro, un filtro métrico y una alarma para deshabilitar o eliminar de forma programada los datos creados por el cliente CMKs	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2	BAJA	 No	Periódico
CloudWatch h8.	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios de política de bucket de S3	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2	BAJA	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudWatch h9.	Asegúrese de que existan un registro métrico, un filtro y una alarma para los cambios AWS Config de configuración	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2	BAJA	 No	Periódico
CloudWatch h1.10	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios de grupos de seguridad	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2	BAJA	 No	Periódico
CloudWatch h1.1	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en las listas de control de acceso a la red (NACL)	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2	BAJA	 No	Periódico
CloudWatch h1.2	Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a las puertas de enlace de la red	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2	BAJA	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudWatch h1.3	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en la tabla de enrutamiento	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2	BAJA	 No	Periódico
CloudWatch h1.4	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en la VPC	CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2	BAJA	 No	Periódico
CloudWatch h1.5	CloudWatch las alarmas deben tener configuradas las acciones especificadas	NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2	ALTO	 Sí	El cambio se ha activado
CloudWatch h1.6	CloudWatch Los grupos de registros deben conservarse durante un período de tiempo específico	NIST SP 800-53 Rev. 5	MEDIO	 Sí	Periódico
CloudWatch h1.7	CloudWatch las acciones de alarma deben estar habilitadas	NIST SP 800-53 Rev. 5	ALTO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CodeArtifact1.	CodeArtifact los repositorios deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
CodeBuild1.	CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, estándar de gestión de servicios: AWS Control Tower	CRÍTICO	 No	El cambio se ha activado
CodeBuild2.	CodeBuild las variables de entorno del proyecto no deben contener credenciales de texto claro	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	CRÍTICO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CodeBuild 3.	CodeBuild Los registros de S3 deben estar cifrados	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios:, AWS Control Tower	BAJA	 No	El cambio se ha activado
CodeBuild 4.	CodeBuild los entornos del proyecto deben tener una configuración de registro	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	MEDIO	 No	El cambio se ha activado
CodeBuild 7.	CodeBuild las exportaciones de los grupos de informes deben estar cifradas en reposo	AWS Mejores prácticas de seguridad fundamentales	MEDIO	 No	El cambio se ha activado
CodeGuruProfiler1.	CodeGuru Los grupos de creación de perfiles de Profiler deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CodeGuruReviewer1.	CodeGuru Las asociaciones de repositorios de Reviewer deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Cognito.1	Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 Sí	El cambio se ha activado
Config.1	AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, AWS AWS Foundational Security Best Practices, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1	CRÍTICO	 Sí	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Conectar.1	Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Conectar.2	Las instancias de Amazon Connect deben tener el CloudWatch registro activado	AWS Mejores prácticas de seguridad fundamentales	MEDIO	 No	El cambio se ha activado
DataFirehose.1	Los flujos de entrega de Firehose deben estar cifrados en reposo	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	 No	Periódico
DataSync1	DataSync las tareas deben tener el registro activado	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 No	El cambio se ha activado
DataSync2	DataSync las tareas deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Detective.1	Los gráficos de comportamiento de Detective deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
DMS.1	Las instancias de replicación de Servicio de migración de bases de datos no deben ser públicas	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	CRÍTICO	 No	Periódico
DMS.2	Los certificados DMS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
DMS.3	Las suscripciones a eventos de DMS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
DMS.4	Las instancias de replicación de DMS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
DMS.5	Los grupos de subredes de replicación del DMS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
DMS.6	Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
DMS.7	Las tareas de replicación del DMS para la base de datos de destino deben tener el registro habilitado	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
DMS.8	Las tareas de replicación del DMS para la base de datos de origen deben tener el registro habilitado	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
DMS.9	Los puntos finales del DMS deben usar SSL	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
DMS.10	Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
DMS.11	Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
DMS.12	Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
DocumentB.1	Los clústeres de Amazon DocumentDB deben estar cifrados en reposo	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Documentación B.2	Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 Sí	El cambio se ha activado
Documentación B.3	Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	CRÍTICO	 No	El cambio se ha activado
Documentación B.4	Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
Documentación B.5	Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Documento DB.6	Los clústeres de Amazon DocumentDB deben cifrarse en tránsito	AWS Prácticas recomendadas de seguridad fundamentales	MEDIO	 No	Periódico
DynamoDB 1	Las tablas de DynamoDB deberían escalar automáticamente la capacidad en función de la demanda	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	MEDIO	 Sí	Periódico
DynamoDB 2	Las tablas de DynamoDB deben tener habilitada la recuperación point-in-time	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
DynamoDB 3	Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
DynamoDB 4	Las tablas de DynamoDB deben estar presentes en un plan de copia de seguridad	NIST SP 800-53 Rev. 5	MEDIO	 Sí	Periódico
DynamoDB 5	Las tablas de DynamoDB deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
DynamoDB 6	Las tablas de DynamoDB deben tener la protección contra eliminación habilitada	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
DynamoDB 7	Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC21.	Las instantáneas de EBS no se deben poder restaurar públicamente	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: PCI DSS v3.2.1, NIST SP 800-53 Rev. 5 AWS Control Tower	CRÍTICO	 No	Periódico
EC22.	Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, estándar de gestión de servicios: PCI DSS v3.2.1, CIS Foundations Benchmark AWS Control Tower v1.4.0, NIST SP 800-53 rev. 5 AWS	ALTO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC23.3	Los volúmenes de EBS asociados deben cifrarse en reposo	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	MEDIO	 No	El cambio se ha activado
EC24.	EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 rev. AWS Control Tower 5	MEDIO	 Sí	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC26.	El registro de flujo de VPC debe estar habilitado en todos VPCs	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, estándar de gestión de servicios: PCI DSS v3.2.1, CIS AWS Foundations Benchmark AWS Control Tower v1.4.0, NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2	MEDIO	 No	Periódico
EC27.	El cifrado predeterminado EBS debe estar habilitado	CIS AWS Foundations Benchmark v3.0.0, AWS Foundational Security Best Practices v1.0.0, Service Managed Standard: CIS AWS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC28.	EC2 las instancias deben usar Instance Metadata Service, versión 2 () IMDSv2	CIS AWS Foundations Benchmark v3.0.0, AWS Foundational Security Best Practices, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO	 No	El cambio se ha activado
EC29.	EC2 las instancias no deben tener una dirección pública IPv4	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower 5	ALTO	 No	El cambio se ha activado
EC21.10	Amazon EC2 debe configurarse para utilizar los puntos de enlace de VPC que se crean para el servicio de Amazon EC2	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de gestión de servicios: NIST SP 800-53 rev. 5 AWS Control Tower, NIST SP 800-171 rev. 2	MEDIO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC21.2	Los que no se usen EC2 EIPs deben ser retirados	PCI DSS v3.2.1, NIST SP 800-53 rev. 5	BAJA	 No	El cambio se ha activado
EC21.3	Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 o ::/0 al puerto 22	CIS AWS Foundations Benchmark v1.2.0, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2	ALTO	 No	El cambio se desencadena y es periódico
EC21.4	Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 o ::/0 al puerto 3389	Índice de referencia CIS AWS Foundations v1.2.0, PCI DSS v4.0.1	ALTO	 No	El cambio se desencadena y es periódico
EC21.5	EC2 las subredes no deberían asignar automáticamente direcciones IP públicas	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios, AWS Control Tower	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC21.6	Deben eliminarse las listas de control de acceso a la red no utilizadas	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2, PCI DSS v4.0.1, estándar de administración de servicios:, AWS Control Tower	BAJA	 No	El cambio se ha activado
EC21.7	EC2 las instancias no deben usar múltiples ENIs	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	BAJA	 No	El cambio se ha activado
EC21.8	Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 rev. 5 AWS Control Tower, NIST SP 800-171 rev. 2	ALTO	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC21.9	Los grupos de seguridad no deben permitir el acceso irrestricto a los puertos de alto riesgo	AWS Mejores prácticas fundamentales de seguridad, estándar de gestión de servicios: NIST SP 800-53 Rev. AWS Control Tower 5, NIST SP 800-171 Rev. 2	CRÍTICO	 No	El cambio se desencadena y es periódico
EC22.0	Los dos túneles VPN de una conexión AWS Site-to-Site VPN deberían estar activos	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 rev. AWS Control Tower 5, NIST SP 800-171 rev. 2	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC22.1	La red no ACLs debe permitir la entrada desde el 0.0.0.0/0 al puerto 22 o al puerto 3389	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, prácticas recomendadas de seguridad AWS fundamentales, estándar de gestión de servicios: NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2 AWS Control Tower, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
EC22.2	Se deben EC2 eliminar los grupos de seguridad no utilizados	Estándar gestionado por el servicio: AWS Control Tower	MEDIO	 No	Periódico
EC22.3	EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 Rev. 5	ALTO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC22.4	EC2 No se deben usar tipos de instancias paravirtuales	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
EC22.5	EC2 las plantillas de lanzamiento no deben asignar interfaces públicas IPs a las de red	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO	 No	El cambio se ha activado
EC22.8	Los volúmenes de EBS tienen que ser parte de un plan de copia de seguridad	NIST SP 800-53 Rev. 5	BAJA	 Sí	Periódico
EC2.33	EC2 Los archivos adjuntos a las pasarelas de tránsito deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC23.4	EC2 Las tablas de rutas de las pasarelas de tránsito deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC23.5	EC2 las interfaces de red deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC23.6	EC2 las pasarelas de los clientes deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC23.7	EC2 Las direcciones IP elásticas deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC23.8	EC2 las instancias deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC2.39	EC2 las pasarelas de internet deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC24.0	EC2 Las pasarelas NAT deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC24.1	EC2 la red ACLs debe estar etiquetada	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC24.2	EC2 las tablas de rutas deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC24.3	EC2 los grupos de seguridad deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC24.4	EC2 las subredes deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC24.5	EC2 los volúmenes deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC24.6	Amazon VPCs debería estar etiquetado	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC24.7	Los servicios de puntos de conexión de Amazon VPC deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC24.8	Los registros de flujo de Amazon VPC deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC24.9	Las conexiones de emparejamiento de Amazon VPC deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC25.0	EC2 Las pasarelas VPN deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC25.1	EC2 Los puntos finales de Client VPN deben tener habilitado el registro de conexiones de clientes	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	BAJA	 No	El cambio se ha activado
EC25.2	EC2 las pasarelas de tránsito deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC25.3	EC2 los grupos de seguridad no deberían permitir la entrada desde 0.0.0.0/0 a los puertos de administración remota del servidor	CIS AWS Foundations Benchmark v3.0.0, PCI DSS v4.0.1	ALTO	 No	Periódico
EC25.4	EC2 los grupos de seguridad no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor	CIS AWS Foundations Benchmark v3.0.0, PCI DSS v4.0.1	ALTO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC25.5	VPCs debe configurarse con un punto final de interfaz para la API ECR	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	 Sí	Periódico
EC25.6	VPCs debe configurarse con un punto final de interfaz para Docker Registry	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	 Sí	Periódico
EC25.7	VPCs debe configurarse con un punto final de interfaz para Systems Manager	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	 Sí	Periódico
EC25.8	VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	 Sí	Periódico
EC26.0	VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	 Sí	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC21.70	EC2 las plantillas de lanzamiento deben usar Instance Metadata Service, versión 2 () IMDSv2	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	BAJA	 No	El cambio se ha activado
EC21.71	EC2 Las conexiones VPN deberían tener el registro activado	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
EC21.72	EC2 La configuración de acceso público del bloque de VPC debería bloquear el tráfico de las puertas de enlace de Internet	AWS Mejores prácticas de seguridad fundamentales	MEDIO	 Sí	El cambio se ha activado
EC21.73	EC2 Las solicitudes de Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 No	El cambio se ha activado
EC21.74	EC2 Los conjuntos de opciones de DHCP deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.175	EC2 las plantillas de lanzamiento deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC2.176	EC2 las listas de prefijos deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC2.177	EC2 las sesiones espejo de tráfico deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC2.178	EC2 Los filtros de los espejos de tráfico deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EC2.179	EC2 Los objetivos de los espejos de tráfico deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ECR.1	Los repositorios privados de ECR deben tener configurado el escaneo de imágenes	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO	 No	Periódico
ECR.2	Los repositorios privados de ECR deben tener configurada la inmutabilidad de las etiquetas	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
ECR.3	Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ECR.4	Los repositorios públicos de ECR deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
ECR.5	Los repositorios de ECR deben estar cifrados y gestionados por el cliente AWS KMS keys	NIST SP 800-53 Rev. 5	MEDIO	 Sí	El cambio se ha activado
ECS.1	Las definiciones de tareas de Amazon ECS deben tener modos de red seguros y definiciones de usuario.	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	ALTO	 No	El cambio se ha activado
ECS.2	Los servicios de ECS no deberían tener direcciones IP públicas asignadas automáticamente	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ECS.3	Las definiciones de tareas de ECS no deben compartir el espacio de nombres del proceso del host	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	ALTO	 No	El cambio se ha activado
ECS.4	Los contenedores ECS deben ejecutarse sin privilegios	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	ALTO	 No	El cambio se ha activado
ECS.5	Los contenedores ECS deben estar limitados a un acceso de solo lectura a los sistemas de archivos raíz	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	ALTO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ECS.8	Los secretos no deben pasarse como variables de entorno del contenedor	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO	 No	El cambio se ha activado
ECS.9	Las definiciones de tareas de ECS deben tener una configuración de registro	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	ALTO	 No	El cambio se ha activado
ECS.10	Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ECS.12	Los clústeres de ECS deben usar Container Insights	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
ECS.13	Los servicios de ECS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
ECS.14	Los clústeres de ECS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
ECS.15	Las definiciones de tareas de ECS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
ECS.16	Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ECS.17	Las definiciones de tareas de ECS no deben utilizar el modo de red host	NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
EFS.1	El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS	CIS AWS Foundations Benchmark v3.0.0, AWS Foundational Security Best Practices v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Periódico
EFS.2	Los volúmenes de Amazon EFS deben estar en los planes de copia de seguridad	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EFS.3	Los puntos de acceso EFS deben aplicar un directorio raíz	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
EFS.4	Los puntos de acceso EFS deben imponer una identidad de usuario	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado
EFS.5	Los puntos de acceso de EFS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EFS.6	Los destinos de montaje de EFS no deben estar asociados a una subred pública	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EFS.7	Los sistemas de archivos de EFS deben tener habilitadas las copias de seguridad automáticas	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 No	El cambio se ha activado
EFS.8	Los sistemas de archivos de EFS deben cifrarse en reposo	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 Sí	El cambio se ha activado
EKS.1	Los puntos de conexión del clúster EKS no deben ser de acceso público	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	 No	Periódico
EKS.2	Los clústeres de EKS deben ejecutarse en una versión compatible de Kubernetes	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EKS.3	Los clústeres de EKS deben usar secretos de Kubernetes cifrados	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	Periódico
EKS.6	Los clústeres de EKS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EKS.7	Las configuraciones de los proveedores de identidad de EKS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EKS.8	Los clústeres de EKS deben tener habilitado el registro de auditoría	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
Elasticache1.	Elasticache Los clústeres (Redis OSS) deben tener habilitadas las copias de seguridad automáticas	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 Rev. 5	ALTO	 Sí	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ElastiCache2.	ElastiCache los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO	 No	Periódico
ElastiCache3.	ElastiCache los grupos de replicación deberían tener habilitada la conmutación por error automática	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Periódico
ElastiCache4.	ElastiCache los grupos de replicación deberían ser encrypted-at-rest	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Periódico
ElastiCache5.	ElastiCache los grupos de replicación deberían ser encrypted-in-transit	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ElastiCache6.	ElastiCache (Redis OSS) los grupos de replicación de versiones anteriores deberían tener habilitada la autenticación de Redis OSS	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	Periódico
ElastiCache7.	ElastiCache los clústeres no deben usar el grupo de subredes predeterminado	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 Rev. 5	ALTO	 No	Periódico
ElasticBeanstalk1.	Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	BAJA	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ElasticBeanstalk2.	Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO	 Sí	El cambio se ha activado
ElasticBeanstalk3.	Elastic Beanstalk debe transmitir los registros a CloudWatch	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	 Sí	El cambio se ha activado
ELB.1	El Equilibrador de carga de aplicación debe configurarse para redirigir todas las solicitudes HTTP a HTTPS	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	MEDIO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ELB.2	Los SSL/HTTPS balanceadores de carga clásicos con oyentes deben usar un certificado proporcionado por AWS Certificate Manager	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 rev. 5 AWS Control Tower, NIST SP 800-171 rev. 2	MEDIO	 No	El cambio se ha activado
ELB.3	Los oyentes de Equilibrador de carga clásico deben configurarse con una terminación HTTPS o TLS	AWS Mejores prácticas fundamentales de seguridad , NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado
ELB.4	Equilibrador de carga de aplicación debe configurarse para eliminar los encabezados http	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ELB.5	El registro de aplicaciones y de los equilibradores de carga clásicos debe estar habilitado	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
ELB.6	La protección contra la eliminación de un equilibrador de carga de aplicación, de puerta de enlace y de red debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad, estándar de gestión de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
ELB.7	Los equilibradores de carga clásicos deberían tener habilitado el drenaje de conexiones	AWS Mejores prácticas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ELB.8	Los equilibradores de carga clásicos con detectores SSL deben usar una política de seguridad predefinida que tenga una configuración sólida	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado
ELB.9	Los equilibradores de carga clásicos deben tener habilitado el equilibrador de carga entre zonas	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
ELB.10	Equilibrador de carga clásico debe abarcar varias zonas de disponibilidad	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ELB.12	Equilibrador de carga de aplicación debe configurarse con el modo defensivo o de mitigación de desincronización más estricto.	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado
ELB.13	Los equilibradores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 Sí	El cambio se ha activado
ELB.14	Equilibrador de carga clásico debe configurarse con el modo defensivo o con el modo de mitigación de desincronización más estricto.	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ELB.16	Los balanceadores de carga de aplicaciones deben estar asociados a una ACL web WAF AWS	NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
ELB.17	Los balanceadores de carga de aplicaciones y redes con oyentes deben usar las políticas de seguridad recomendadas	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
EMR.1	Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO	 No	Periódico
EMR.2	La configuración de bloqueo del acceso público de Amazon EMR debe estar habilitada	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	CRÍTICO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EMR.3	Las configuraciones de seguridad de Amazon EMR deben estar cifradas en reposo	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
EMR. 4	Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
ES.1	Los dominios de Elasticsearch deben tener habilitado el cifrado en reposo	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: PCI DSS v3.2.1, NIST SP 800-53 rev. AWS Control Tower 5	MEDIO	 No	Periódico
ES.2	Los dominios de Elasticsearch no deben ser de acceso público	AWS Mejores prácticas de seguridad fundamentales, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5, estándar de administración de servicios: AWS Control Tower	CRÍTICO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ES.3	Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 rev. 5, PCI DSS v4.0.1, estándar de administración de servicios:, AWS Control Tower	MEDIO	 No	El cambio se ha activado
ES.4	El registro de CloudWatch errores del dominio de Elasticsearch en Logs debe estar habilitado	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
ES.5	Los dominios de Elasticsearch deben tener habilitado el registro de auditoría	AWS Mejores prácticas fundamentales de seguridad , NIST SP 800-53 Rev. 5, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ES.6	Los dominios de Elasticsearch deben tener al menos tres nodos de datos	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
ES.7	Los dominios de Elasticsearch deben configurarse con al menos tres nodos maestros dedicados	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
ES.8	Las conexiones a dominios de Elasticsearch deben estar cifradas conforme a la política de seguridad TLS más reciente	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ES.9	Los dominios de Elasticsearch deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EventBridge2.	EventBridge los autobuses del evento deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
EventBridge3.	EventBridge los autobuses personalizados para eventos deberían tener adjunta una política basada en los recursos	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	BAJA	 No	El cambio se ha activado
EventBridge4.	EventBridge los puntos finales globales deberían tener habilitada la replicación de eventos	NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
FraudDetector1.	Los tipos de entidad de Amazon Fraud Detector deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
FraudDetector2.	Las etiquetas de Amazon Fraud Detector deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
FraudDetector3.	Los resultados de Amazon Fraud Detector deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
FraudDetector4.	Las variables de Amazon Fraud Detector deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
FSx1.	FSx para los sistemas de archivos OpenZFS, debe configurarse para copiar etiquetas en copias de seguridad y volúmenes	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	BAJA	 No	Periódico
FSx2.	FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	BAJA	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
FSx3.	FSx para los sistemas de archivos OpenZFS, debe configurarse para el despliegue en zonas de disponibilidad múltiples	AWS Mejores prácticas de seguridad fundamentales	MEDIO	 No	Periódico
FSx4.	FSx para los sistemas de archivos NetApp ONTAP, debe configurarse para el despliegue en zonas de disponibilidad múltiples	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 Sí	Periódico
FSx5.	FSx para los sistemas de archivos del servidor de archivos de Windows, debe configurarse para la implementación en zonas de disponibilidad múltiples	AWS Prácticas recomendadas de seguridad fundamentales	MEDIO	 No	Periódico
Glue.1	AWS Glue los trabajos deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Glue.3	AWS Glue Las transformaciones de aprendizaje automático o deben cifrarse en reposo	AWS Mejores prácticas de seguridad fundamentales	MEDIO	 No	El cambio se ha activado
Pegamento.4	AWS Glue Los trabajos de Spark deberían ejecutarse en versiones compatibles de AWS Glue	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
GlobalAccelerator1.	Los aceleradores de Global Accelerator deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
GuardDuty1.	GuardDuty debe estar activado	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
GuardDuty 4.2.	GuardDuty los filtros deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
GuardDuty 3.	GuardDuty IPSets debe estar etiquetado	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
GuardDuty 4.	GuardDuty los detectores deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
GuardDuty 5.	GuardDuty La supervisión del registro de auditoría de EKS debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad	ALTO	 No	Periódico
GuardDuty 6.	GuardDuty La protección Lambda debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	 No	Periódico
GuardDuty 7.	GuardDuty La monitorización del tiempo de ejecución de EKS debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	MEDIO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
GuardDuty 8.	GuardDuty La protección contra malware para EC2 debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad	ALTO	 No	Periódico
GuardDuty 9.	GuardDuty La protección RDS debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	 No	Periódico
GuardDuty .10	GuardDuty La protección S3 debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	 No	Periódico
GuardDuty 1.1	GuardDuty La supervisión del tiempo de ejecución debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad	ALTO	 No	Periódico
GuardDuty 1.2	GuardDuty La supervisión del tiempo de ejecución de ECS debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 No	Periódico
GuardDuty 1.3	GuardDuty EC2 La supervisión del tiempo de ejecución debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.1	Las políticas de IAM no deben permitir privilegios administrativos completos “*”	CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, estándar de administración de servicios: PCI DSS v3.2.1, CIS AWS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2	ALTO	 No	El cambio se ha activado
IAM.2	Los usuarios de IAM no deben tener políticas de IAM asociadas	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.2.0, Foundational Security Best Practices v1.0.0 AWS Control Tower, estándar de administración de servicios: PCI DSS v3.2.1, NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2	BAJA	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.3	Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS AWS Foundations Benchmark v1.2.0, Foundational Security Best Practices, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	Periódico
IAM.4	La clave de acceso del usuario raíz de IAM no debería existir	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS AWS Foundations Benchmark v1.2.0, Foundational Security Best Practices v1.0.0 AWS Control Tower, Estándar de gestión de servicios: PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	CRÍTICO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.5	MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS AWS Foundations Benchmark v1.2.0, Foundational Security Best Practices, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	Periódico
IAM.6	La MFA de hardware debe estar habilitada para el usuario raíz	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS AWS Foundations Benchmark v1.2.0, Foundational Security Best Practices, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	CRÍTICO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.7	Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 Sí	Periódico
IAM.8	Deben eliminarse las credenciales de usuario de IAM que no se utilicen	CIS AWS Foundations Benchmark v1.2.0, prácticas recomendadas de seguridad AWS fundamentales, NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.9	La MFA debe estar habilitada para el usuario raíz	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	CRÍTICO	 No	Periódico
IAM.10	Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras	NIST SP 800-171 rev. 2, PCI DSS v3.2.1	MEDIO	 No	Periódico
IAM.11	Asegurar que la política de contraseñas de IAM requiere al menos una letra mayúscula	CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2, PCI DSS v4.0.1	MEDIO	 No	Periódico
IAM.12	Asegurar que la política de contraseñas de IAM requiere al menos una letra minúscula	CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2, PCI DSS v4.0.1	MEDIO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.13	Asegurar que la política de contraseñas de IAM requiere al menos un símbolo	CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2, PCI DSS v4.0.1	MEDIO	 No	Periódico
IAM.14	Asegurar que la política de contraseñas de IAM requiere al menos un número	CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2, PCI DSS v4.0.1	MEDIO	 No	Periódico
IAM.15	Asegurar que la política de contraseñas de IAM requiere una longitud mínima de 14 o más	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2 AWS	MEDIO	 No	Periódico
IAM.16	Asegurar que la política de contraseñas de IAM impide la reutilización de contraseñas	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2, PCI DSS v4.0.1 AWS	BAJA	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.17	Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos	CIS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2, PCI DSS v4.0.1 AWS	BAJA	 No	Periódico
IAM.18	Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-171 rev. 2, PCI DSS v4.0.1 AWS	BAJA	 No	Periódico
IAM.19	MFA se debe habilitar para todos los usuarios de IAM	NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	MEDIO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.21	Las políticas de IAM administrada por los clientes que usted cree no deberían permitir acciones comodín para los servicios	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, estándar de administración de servicios: NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2 AWS Control Tower	BAJA	 No	El cambio se ha activado
IAM.22	Deben eliminarse las credenciales de usuario de IAM que no se hayan utilizado durante 45 días	CIS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-171 rev. 2 AWS	MEDIO	 No	Periódico
IAM.23	Los analizadores del Analizador de acceso de IAM deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
IAM.24	Los roles de IAM deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.25	Los usuarios de IAM deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
IAM.26	SSL/TLS Los certificados caducados gestionados en IAM deben eliminarse	CIS AWS Foundations Benchmark v3.0.0	MEDIO	 No	Periódico
IAM.27	Las identidades de IAM no deberían tener la política adjunta AWSCloud ShellFull Access	CIS AWS Foundations Benchmark v3.0.0	MEDIO	 No	El cambio se ha activado
IAM.28	El analizador de acceso externo del Analizador de acceso de IAM debe estar habilitado	Punto de referencia sobre AWS fundacion es CIS v3.0.0	ALTO	 No	Periódico
Inspector .1	El EC2 escaneo de Amazon Inspector debe estar activado	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	 No	Periódico
Inspector .2	El análisis de ECR en Amazon Inspector debe estar habilitado	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Inspector .3	El análisis de código de Lambda en Amazon Inspector debe estar habilitado	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	 No	Periódico
Inspector .4	El análisis de estándar de Lambda en Amazon Inspector debe estar habilitado	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	 No	Periódico
IoT.1	AWS IoT Device Defender los perfiles de seguridad deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
IoT.2	AWS IoT Core las acciones de mitigación deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
IoT.3	AWS IoT Core las dimensiones deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
IoT.4	AWS IoT Core los autorizadores deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IoT.5	AWS IoT Core Los alias de los roles deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
IoT.6	AWS IoT Core las políticas deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
iOS 1.1 TEvents	AWS IoT Events las entradas deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
iOS 1.2 TEvents	AWS IoT Events los modelos de detectores deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
iOS 1.3 TEvents	AWS IoT Events los modelos de alarma deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Io Wise.1 TSite	AWS IoT SiteWise los modelos de activos deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Io Wise.2 TSite	AWS IoT SiteWise los cuadros de mando deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Io Wise.3 TSite	AWS IoT SiteWise las pasarelas deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Io Wise.4 TSite	AWS IoT SiteWise los portales deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Io Wise.5 TSite	AWS IoT SiteWise los proyectos deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Io Maker.1 TTwin	AWS Los trabajos de TwinMaker sincronización de IoT deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Io Maker.2 TTwin	AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IoT Maker.3 TTwin	AWS TwinMaker Las escenas de IoT deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
IoT Maker TTwin n. 4	AWS TwinMaker Las entidades de IoT deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
iOS 1.1 TWireless	AWS Los grupos de multidifusión de IoT Wireless deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
iOS 1.2 TWireless	AWS Los perfiles del servicio IoT Wireless deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
iOS 1.3 TWireless	AWS Las tareas de IoT Wireless FUOTA deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
IVS.1	Los pares de claves de reproducción del IVS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IVS.2	Las configuraciones de grabación del IVS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
IVS.3	Los canales IVS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Espacios clave. 1	Los espacios clave de Amazon Keyspaces deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Kinesis.1	Las transmisiones de Kinesis deben cifrarse en reposo	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
Kinesis.2	Las transmisiones de Kinesis deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Kinesis.3	Las transmisiones de Kinesis deben tener un periodo adecuado de retención de datos	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 Sí	El cambio se ha activado
KMS.1	Las políticas administradas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
KMS.2	Las entidades principales de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
KMS.3	AWS KMS keys no debe eliminarse involuntariamente	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	CRÍTICO	 No	El cambio se ha activado
KMS.4	AWS KMS key la rotación debe estar habilitada	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v1.2.0, NIST SP 800-53 rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	MEDIO	 No	Periódico
KMS.5	Las claves KMS no deben ser de acceso público	AWS Mejores prácticas fundamentales de seguridad	CRÍTICO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Lambda.1	Las funciones de Lambda deberían prohibir el acceso público	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	CRÍTICO	 No	El cambio se ha activado
Lambda.2	Las funciones de Lambda deben usar los últimos tiempos de ejecución	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado
Lambda.3	Las funciones de Lambda deben estar en una VPC	PCI DSS v3.2.1, NIST SP 800-53 rev. 5	BAJA	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Lambda.5	Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 Sí	El cambio se ha activado
Lambda.6	Las funciones de Lambda deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Macie.1	Amazon Macie debe estar habilitado	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Periódico
Macie.2	La detección automática de datos confidenciales de Macie debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	ALTO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
MSK.1	Los clústeres de MSK deben cifrarse en tránsito entre los nodos de los corredores	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
MSK.2	Los clústeres de MSK deberían tener configurada una supervisión mejorada	NIST SP 800-53 Rev. 5	BAJA	 No	El cambio se ha activado
MSK.3	Los conectores de MSK Connect deben cifrarse en tránsito	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	MEDIO	 no	El cambio se ha activado
MQ.2	Los corredores de ActiveMQ deben transmitir los registros de auditoría a CloudWatch	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
MQ.3	Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	BAJA	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
MQ.4	Los agentes de Amazon MQ deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
MQ.5	Los corredores de ActiveMQ deberían usar el modo de implementación active/standby	NIST SP 800-53 Rev. 5, estándar de administración de servicios: AWS Control Tower	BAJA	 No	El cambio se ha activado
MQ.6	Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres	NIST SP 800-53 Rev. 5, estándar de administración de servicios: AWS Control Tower	BAJA	 No	El cambio se ha activado
Neptune.1	Los clústeres de bases de datos de Neptune deberían estar cifrados en reposo	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Neptune.2	Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado
Neptune.3	Las instantáneas del clúster de base de datos de Neptune no deben ser públicas	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	CRÍTICO	 No	El cambio se ha activado
Neptune.4	Los clústers de Neptune DB deben tener habilitada la protección contra eliminación.	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, estándar de administración de servicios: AWS Control Tower	BAJA	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Neptune.5	Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automatizadas	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 rev. 5, estándar de administración de servicios: AWS Control Tower	MEDIO	 Sí	El cambio se ha activado
Neptune.6	Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 rev. 5, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado
Neptune.7	Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 rev. 5, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Neptune.8	Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 rev. 5, estándar de administración de servicios: AWS Control Tower	BAJA	 No	El cambio se ha activado
Neptune.9	Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad	NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
NetworkFirewall1.	Los firewalls de Network Firewall se deben implementar en varias zonas de disponibilidad	NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
NetworkFirewall2.	El registro de Network Firewall debe estar habilitado	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2	MEDIO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
NetworkFirewall3.	Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 rev. 5 AWS Control Tower, NIST SP 800-171 rev. 2	MEDIO	 No	El cambio se ha activado
NetworkFirewall4.	La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos.	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
NetworkFirewall5.	La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados.	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 rev. 5 AWS Control Tower, NIST SP 800-171 rev. 2	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
NetworkFirewall6.	El grupo de reglas de firewall de redes sin estado no debe estar vacío	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 rev. 5 AWS Control Tower, NIST SP 800-171 rev. 2	MEDIO	 No	El cambio se ha activado
NetworkFirewall7.	Los firewall de Network Firewall deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
NetworkFirewall8.	Las políticas de firewall de Network Firewall deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
NetworkFirewall9.	Los firewalls de Network Firewall deben tener habilitada la protección de eliminación	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
NetworkFirewall1.0	Los firewalls de Network Firewall deben tener habilitada la protección contra cambios de subred	AWS Prácticas recomendadas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Opensearch h.1	OpenSearch los dominios deben tener habilitada la encriptación en reposo	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
Opensearch h.2	OpenSearch los dominios no deben ser de acceso público	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	CRÍTICO	 No	El cambio se ha activado
Opensearch h.3	OpenSearch los dominios deben cifrar los datos enviados entre nodos	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Opensearch h.4	OpenSearch El registro de errores de dominio en Logs debe estar habilitado CloudWatch	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	MEDIO	 No	El cambio se ha activado
Opensearch h.5	OpenSearch los dominios deben tener habilitado el registro de auditoría	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado
Opensearch h.6	OpenSearch los dominios deben tener al menos tres nodos de datos	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Opensearch h.7	OpenSearch los dominios deben tener habilitado un control de acceso detallado	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	ALTO	 No	El cambio se ha activado
Opensearch h.8	Las conexiones a los OpenSearch dominios deben cifrarse mediante la última política de seguridad de TLS	AWS Mejores prácticas fundamentales de seguridad, estándar de gestión de servicios: NIST SP 800-53 AWS Control Tower Rev. 5	MEDIO	 No	El cambio se ha activado
Opensearch h.9	OpenSearch los dominios deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Opensearch h.10	OpenSearch los dominios deben tener instalada la última actualización de software	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	BAJA	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Opensearch.h.11	OpenSearch los dominios deben tener al menos tres nodos principales dedicados	NIST SP 800-53 Rev. 5	BAJA	 No	Periódico
PCA.1	AWS Private CA la autoridad de certificación raíz debe estar deshabilitada	AWS Prácticas recomendadas fundamentales de seguridad, versión 1.0.0, NIST SP 800-53 Rev. 5	BAJA	 No	Periódico
PCA.2	AWS Las autoridades certificadoras de CA privadas deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
RDS.1	Las instantáneas de RDS deben ser privadas	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 rev. 5	CRÍTICO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.2	Las instancias de base de datos RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible	CIS AWS Foundations Benchmark v3.0.0, prácticas recomendadas de seguridad AWS fundamentales, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower, PCI DSS v3.2.1, PCI DSS v4.0.1	CRÍTICO	 No	El cambio se ha activado
RDS.3	Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, Foundational Security Best Practices v1.0.0, estándar de gestión de servicios: NIST SP 800-53 AWS rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.4	Las instantáneas del clúster de RDS y las instantáneas de las bases de datos deben cifrarse en reposo	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
RDS.5	Las instancias de base de datos de RDS deben configurarse con varias zonas de disponibilidad	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
RDS.6	Se debe configurar una supervisión mejorada para las instancias de base de datos de RDS	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.7	Los clústeres RDS deben tener habilitada la protección contra la eliminación	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	BAJA	 No	El cambio se ha activado
RDS.8	Indica si las instancias de base de datos de RDS debe tener la protección contra eliminación habilitada.	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	BAJA	 No	El cambio se ha activado
RDS.9	Las instancias de base de datos de RDS deben publicar registros en Logs CloudWatch	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.10	La autenticación de IAM debe configurarse para las instancias de RDS	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
RDS.11	Las instancias RDS deben tener habilitadas las copias de seguridad automáticas	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 Sí	El cambio se ha activado
RDS.12	La autenticación de IAM debe configurarse para los clústeres de RDS	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.13	Deben habilitarse las actualizaciones automáticas entre versiones secundarias de RDS	CIS AWS Foundations Benchmark v3.0.0, prácticas recomendadas de seguridad AWS fundamentales, NIST SP 800-53 rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO	 No	El cambio se ha activado
RDS.14	Los clústeres de Amazon Aurora deben tener habilitada la característica de búsqueda de datos anteriores	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 Sí	El cambio se ha activado
RDS.15	Los clústeres de bases de datos de RDS deben configurarse para varias zonas de disponibilidad	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
RDS.16	Los clústeres de bases de datos de RDS deben configurarse para copiar etiquetas en las instantáneas	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	BAJA	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.17	Las instancias de base de datos de RDS deben configurarse para copiar etiquetas en las instantáneas	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	BAJA	 No	El cambio se ha activado
RDS.18	Las instancias de RDS deben implementarse en una VPC	Estándar de administración de servicios: AWS Control Tower	ALTO	 No	El cambio se ha activado
RDS.19	Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos del clúster	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	BAJA	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.20	Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos de las instancias de bases de datos	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	BAJA	 No	El cambio se ha activado
RDS.21	Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos críticos de los grupos de parámetros de bases de datos	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	BAJA	 No	El cambio se ha activado
RDS.22	Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos críticos de los grupos de seguridad de bases de datos	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	BAJA	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.23	Las instancias RDS no deben usar el puerto predeterminado de un motor de base de datos	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	BAJA	 No	El cambio se ha activado
RDS.24	Los clústeres de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
RDS.25	Las instancias de bases de datos de RDS deben usar un nombre de usuario de administrador personalizado	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado
RDS.26	Las instancias de base de datos de RDS tienen que ser protegidas por planes de copia de seguridad	NIST SP 800-53 Rev. 5	MEDIO	 Sí	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.27	Los clústeres de bases de datos de RDS deben cifrarse en reposo	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado
RDS.28	Los clústeres de base de datos de RDS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
RDS.29	Las instantáneas del clúster de base de datos de RDS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
RDS.30	Las instancias de bases de datos de RDS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
RDS.31	Los grupos de seguridad de bases de datos de RDS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.32	Las instantáneas de bases de datos de RDS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
RDS.33	Los grupos de subredes de bases de datos de RDS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
RDS.34	Los clústeres de bases de datos Aurora MySQL deberían publicar los registros de auditoría en CloudWatch Logs	AWS Prácticas recomendadas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
RDS.35	Los clústeres de bases de datos de RDS deberían tener habilitada la actualización automática de las versiones secundarias	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
RDS.36	Las instancias de base de datos de RDS para PostgreSQL deberían publicar registros en Logs CloudWatch	AWS Prácticas recomendadas fundamentales de seguridad, PCI DSS v4.0.1	MEDIO	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.37	Los clústeres de bases de datos Aurora PostgreSQL deberían publicar registros en Logs CloudWatch	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado
RDS.38	Las instancias de base de datos de RDS para PostgreSQL deben cifrarse en tránsito	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 No	Periódico
RDS.39	Las instancias de base de datos de RDS para MySQL deben cifrarse en tránsito	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 No	Periódico
RDS.40	Las instancias de base de datos de RDS para SQL Server deben publicar los registros en Logs CloudWatch	AWS Prácticas recomendadas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	 Sí	El cambio se ha activado
RDS.41	Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RDS.42	Las instancias de base de datos de RDS para MariaDB deberían publicar registros en Logs CloudWatch	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	 Sí	Periódico
RDS.44	El RDS para las instancias de base de datos MariaDB debe cifrarse en tránsito	AWS Mejores prácticas de seguridad fundamentales	MEDIO	 No	Periódico
Redshift.1	Los clústeres de Amazon Redshift deberían prohibir el acceso público	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	CRÍTICO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Redshift. 2	Las conexiones a los clústeres de Amazon Redshift deben cifrarse en tránsito	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado
Redshift. 3	Los clústeres de Amazon Redshift deben tener habilitadas las instantáneas automáticas	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 Sí	El cambio se ha activado
Redshift. 4	Los clústeres de Amazon Redshift deben tener habilitado el registro de auditoría	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Redshift. 6	Amazon Redshift debería tener habilitadas las actualizaciones automáticas a las versiones principales	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
Redshift. 7	Los clústeres de Redshift deberían utilizar un enrutamiento de VPC mejorado	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
Redshift. 8	Los clústeres de Amazon Redshift no deben usar el nombre de usuario de administrador predeterminado	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Redshift. 9	Los clústeres de Redshift no deben usar el nombre de base de datos predeterminado	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
Redshift. 10	Los clústeres de Redshift deben estar cifrados en reposo	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	El cambio se ha activado
Redshift. 11	Los clústeres de Redshift deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Redshift. 12	Las suscripciones a notificaciones de eventos de Redshift deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Redshift. 13	Las instantáneas del clúster de Redshift deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Redshift. 14	Los grupos de subredes del clúster de Redshift deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Redshift. 15	Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	 No	Periódico
Redshift. 16	Los grupos de subredes de clústeres de Redshift deben tener subredes de varias zonas de disponibilidad	NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
Redshift. 17	Los grupos de parámetros del clúster de Redshift deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RedshiftServerless 1.	Los grupos de trabajo sin servidor de Amazon Redshift deberían utilizar un enrutamiento de VPC mejorado	AWS Prácticas recomendadas de seguridad fundamentales	ALTO	 No	Periódico
RedshiftServerless 2.	Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 No	Periódico
RedshiftServerless 3.	Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público	AWS Mejores prácticas fundamentales de seguridad	ALTO	 No	Periódico
RedshiftServerless 4.	Los espacios de nombres de Redshift Serverless deben estar cifrados y gestionados por el cliente AWS KMS keys	NIST SP 800-53 Rev. 5	MEDIO	 Sí	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
RedshiftServerless 5.	Los espacios de nombres Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 Sí	Periódico
RedshiftServerless 6.	Los espacios de nombres Redshift Serverless deberían exportar los registros a los registros CloudWatch	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 No	Periódico
RedshiftServerless 7.	Los espacios de nombres Redshift Serverless no deben usar el nombre de base de datos predeterminado	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	 No	Periódico
Route53.1	Las comprobaciones de estado de Route 53 deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Route53.2	Las zonas alojadas públicas de Route 53 deben registrar las consultas de DNS	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
S3.1	Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, AWS Foundational Security Best Practices, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	Periódico
S3.2	Los buckets de uso general de S3 deben bloquear el acceso público de lectura	AWS Mejores prácticas fundamentales de seguridad, estándar de gestión de servicios: PCI DSS v3.2.1, NIST SP 800-53 Rev. 5 AWS Control Tower	CRÍTICO	 No	El cambio se desencadena y es periódico
S3.3	Los buckets de uso general de S3 deben bloquear el acceso público de escritura	AWS Mejores prácticas fundamentales de seguridad, estándar de administración de servicios: PCI DSS v3.2.1, NIST SP 800-53 Rev. 5 AWS Control Tower	CRÍTICO	 No	El cambio se desencadena y es periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
S3.5	En las solicitudes de los buckets de uso general de S3, se debe pedir el uso de SSL	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, AWS Foundational Security Best Practices, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado
S3.6	Las políticas de compartimentos de uso general de S3 deberían restringir el acceso a otras Cuentas de AWS	AWS Mejores prácticas fundamentales de seguridad, estándar de gestión de servicios: NIST SP 800-53 rev. 5 AWS Control Tower, NIST SP 800-171 rev. 2	ALTO	 No	El cambio se ha activado
S3.7	Los buckets de uso general de S3 deben usar la replicación entre regiones	PCI DSS v3.2.1, NIST SP 800-53 rev. 5	BAJA	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
S3.8	Los buckets de uso general de S3 deben bloquear el acceso público	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, AWS AWS Foundational Security Best Practices, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO	 No	El cambio se ha activado
S3.9	Los buckets de uso general de S3 deben tener habilitado el registro de acceso al servidor	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado
S3.10	Los buckets de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida	NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
S3.11	Los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos	NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2	MEDIO	 Sí	El cambio se ha activado
S3.12	ACLs no debe usarse para administrar el acceso de los usuarios a los depósitos de uso general de S3	AWS Mejores prácticas de seguridad fundamentales, estándar de gestión de servicios: NIST SP 800-53 AWS Control Tower Rev. 5	MEDIO	 No	El cambio se ha activado
S3.13	Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida	AWS Mejores prácticas fundamentales de seguridad, estándar de gestión de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	BAJA	 Sí	El cambio se ha activado
S3.14	Los buckets de uso general de S3 deben tener habilitado el control de versiones	NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2	BAJA	 No	El cambio se ha activado
S3.15	Los buckets de uso general de S3 deben tener habilitado el bloqueo de objetos	NIST SP 800-53 rev. 5, PCI DSS v4.0.1	MEDIO	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
S3.17	Los depósitos de uso general de S3 deben cifrarse en reposo con AWS KMS keys	NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado
S3.19	Los puntos de acceso de S3 deben tener habilitada la configuración de Bloqueo de acceso público	AWS Prácticas recomendadas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	CRÍTICO	 No	El cambio se ha activado
S3.20	Los buckets de uso general de S3 deben tener habilitada la eliminación de MFA	CIS AWS Foundations Benchmark v3.0.0, CIS Foundations Benchmark v1.4.0, NIST SP 800-53 rev. 5 AWS	BAJA	 No	El cambio se ha activado
S3.22	Los buckets de uso general de S3 deben registrar eventos de escritura a nivel de objeto	CIS Foundations Benchmark v3.0.0 AWS , PCI DSS v4.0.1	MEDIO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
S3.23	Los buckets de uso general de S3 deben registrar eventos de lectura a nivel de objeto	Índice de referencia CIS AWS Foundations v3.0.0, PCI DSS v4.0.1	MEDIO	 No	Periódico
S3.24	Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	ALTO	 No	El cambio se ha activado
SageMaker 1.	Las instancias de Amazon SageMaker Notebook no deben tener acceso directo a Internet	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO	 No	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SageMaker 2.	SageMaker las instancias de notebook deben lanzarse en una VPC personalizada	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	ALTO	 No	El cambio se ha activado
SageMaker 3.	Los usuarios no deberían tener acceso root a las instancias de los SageMaker portátiles	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	ALTO	 No	El cambio se ha activado
SageMaker 4.	SageMaker las variantes de producción de terminales deben tener un recuento inicial de instancias superior a 1	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	 No	Periódico
SageMaker 5.	SageMaker los modelos deberían bloquear el tráfico entrante	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SageMaker 6.	SageMaker las configuraciones de imagen de la aplicación deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
SageMaker 7.	SageMaker las imágenes deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
SageMaker 8.	SageMaker las instancias de notebook deberían ejecutarse en plataformas compatibles	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 No	Periódico
SecretsManager1.	Los secretos de Secrets Manager deberían tener habilitada la rotación automática	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SecretsManager2.	Los secretos de Secrets Manager configurados con rotación automática deberían rotar correctamente	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 No	El cambio se ha activado
SecretsManager3.	Eliminación de secretos no utilizados de Secrets Manager	AWS Mejores prácticas de seguridad fundamentales, NIST SP 800-53 Rev. 5, estándar de gestión de servicios: AWS Control Tower	MEDIO	 Sí	Periódico
SecretsManager4.	Los secretos de Secrets Manager deben rotarse en un número específico de días	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	 Sí	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SecretsManager5.	Los secretos de Secrets Manager deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
ServiceCatalog1.	Las carteras de Service Catalog solo deben compartirse dentro de una AWS organización	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	ALTO	 No	Periódico
SES.1	Las listas de contactos de SES deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
SES.2	Los conjuntos de configuración de SES deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
SNS.1	Los temas de SNS deben cifrarse en reposo mediante AWS KMS	NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2	MEDIO	 No	El cambio se ha activado
SNS.3	Los temas de SNS deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SNS.4	Las políticas de acceso a los temas de SNS no deberían permitir el acceso público	AWS Mejores prácticas fundamentales de seguridad	ALTO	 No	El cambio se ha activado
SQS.1	Las colas de Amazon SQS deben cifrarse en reposo	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
SQS.2	Las colas de SQS deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
SQS.3	Las políticas de acceso a las colas de SQS no deberían permitir el acceso público	AWS Mejores prácticas fundamentales de seguridad	ALTO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SSM.1	EC2 las instancias deben ser administradas por AWS Systems Manager	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
SSM.2	EC2 las instancias administradas por Systems Manager deben tener un estado de conformidad con los parches de CONFORMIDAD tras la instalación de un parche	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 rev. 5, NIST SP 800-171 rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO	 No	El cambio se ha activado
SSM.3	EC2 las instancias administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT	AWS Prácticas recomendadas de seguridad fundamentales, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1, estándar de gestión de servicios: AWS Control Tower	BAJA	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
SSM.4	Los documentos del SSM no deben ser públicos	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	CRÍTICO	 No	Periódico
SSM.5	Los documentos SSM deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
StepFunctions1.	Step Functions indica que las máquinas deberían tener el registro activado	AWS Mejores prácticas fundamentales de seguridad, PCI DSS v4.0.1	MEDIO	 Sí	El cambio se ha activado
StepFunctions2.	Las actividades de Step Functions deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Transfer.1	Los flujos de trabajo de Transfer Family deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Transferencia.2	Los servidores de Transfer Family no deben utilizar el protocolo FTP para la conexión del punto de conexión	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	Periódico
Transferencia.3	Los conectores de Transfer Family deben tener habilitado el registro	AWS Mejores prácticas fundamentales de seguridad, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
Transferencia.4	Los acuerdos de Transfer Family deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Transferencia.5	Los certificados de Transfer Family deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
Transferencia.6	Los conectores de Transfer Family deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Transferencia.7	Los perfiles de Transfer Family deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	 Sí	El cambio se ha activado
WAF.1	AWS El registro de ACL web global de WAF Classic debe estar habilitado	AWS Prácticas recomendadas fundamentales de seguridad, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO	 No	Periódico
WAF.2	AWS Las reglas regionales clásicas de la WAF deben tener al menos una condición	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de gestión de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
WAF.3	AWS Los grupos de reglas regionales clásicas de WAF deben tener al menos una regla	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 rev. 5	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
WAF.4	AWS La web ACLs WAF Classic Regional debe tener al menos una regla o grupo de reglas	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
WAF.6	AWS Las reglas globales de WAF Classic deben tener al menos una condición	AWS Prácticas recomendadas fundamentales de seguridad, versión 1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
WAF.7	AWS Los grupos de reglas globales de WAF Classic deben tener al menos una regla	AWS Prácticas recomendadas fundamentales de seguridad, versión 1.0.0, NIST SP 800-53 rev. 5	MEDIO	 No	El cambio se ha activado
WAF.8	AWS La web global de WAF Classic ACLs debe tener al menos una regla o grupo de reglas	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
WAF.10	AWS La web WAF ACLs debe tener al menos una regla o grupo de reglas	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	MEDIO	 No	El cambio se ha activado
WAF.11	AWS El registro de ACL web en WAF debe estar habilitado	NIST SP 800-53 rev. 5, PCI DSS v4.0.1	BAJA	 No	Periódico
WAF.12	AWS Las reglas WAF CloudWatch deben tener las métricas habilitadas	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	MEDIO	 No	El cambio se ha activado
WorkSpaces1.	WorkSpaces los volúmenes de usuario deben cifrarse en reposo	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 No	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
WorkSpaces2.	WorkSpaces los volúmenes raíz deben cifrarse en reposo	AWS Mejores prácticas fundamentales de seguridad	MEDIO	 No	El cambio se ha activado

Registro de cambios para los controles CSPM de Security Hub

El siguiente registro de cambios registra los cambios importantes en los controles de AWS seguridad existentes de Security Hub Cloud Security Posture Management (CSPM), que pueden provocar cambios en el estado general de un control y en el estado de cumplimiento de sus hallazgos.

Para obtener información sobre cómo Security Hub CSPM evalúa el estado del control, consulte.

[Evaluación del estado de cumplimiento y el estado de control](#) Los cambios pueden tardar unos días después de su entrada en este registro y afectar a todas las unidades Regionales de AWS en las que esté disponible el control.

Este registro realiza el seguimiento de los cambios que se han producido desde abril de 2023. Elija un control para ver detalles adicionales sobre él. Los cambios de título se anotan en la descripción detallada del control durante 90 días.

Fecha del cambio	ID y título de control	Descripción del cambio
30 de mayo de 2025	[IAM.10] Las políticas de contraseñas de usuarios de IAM deben tener configuraciones seguras	Security Hub CSPM eliminó este control del estándar PCI DSS v4.0.1 . Este control comprueba si las políticas de contraseñas de las cuentas de los usuarios de

Fecha del cambio	ID y título de control	Descripción del cambio
		IAM cumplen los requisitos mínimos, incluida una longitud mínima de contraseñas de 7 caracteres. La versión 4.0.1 de PCI DSS ahora requiere que las contraseñas tengan un mínimo de 8 caracteres. El control sigue aplicándose al estándar PCI DSS v3.2.1, que tiene diferentes requisitos de contraseña. Para evaluar las políticas de contraseñas de las cuentas con respecto a los requisitos de la versión 4.0.1 del PCI DSS, puede utilizar el control IAM.7. Este control requiere que las contraseñas tengan un mínimo de 8 caracteres. También admite valores personalizados para la longitud de la contraseña y otros parámetros. El

Fecha del cambio	ID y título de control	Descripción del cambio
		control IAM.7 forma parte del estándar PCI DSS v4.0.1 del Security Hub CSPM.
8 de mayo de 2025	[RDS.46] Las instancias de base de datos RDS no deben implementarse en subredes públicas con rutas a puertas de enlace de Internet	Security Hub CSPM anuló por completo la versión del control RDS.46. Regiones de AWS Anteriormente, este control era compatible con el estándar AWS Foundational Security Best Practices (FSBP).

Fecha del cambio	ID y título de control	Descripción del cambio
7 de abril de 2025	[ELB.17] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas	Este control comprueba si el agente de escucha HTTPS de un Application Load Balancer o el agente de escucha TLS de un Network Load Balancer están configurados para cifrar los datos en tránsito mediante una política de seguridad recomendada. Security Hub CSPM ahora admite dos valores de parámetros adicionales para este control: <code>ELBSecurityPolicy-TLS13-1-2-Res-2021-06</code> y <code>ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04</code>

Fecha del cambio	ID y título de control	Descripción del cambio
27 de marzo de 2025	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos	Este control comprueba si la configuración del tiempo de ejecución de una AWS Lambda función coincide con los valores esperados para los tiempos de ejecución admitidos en cada idioma. Security Hub CSPM ahora admite ruby3.4 como valor de parámetro para este control. AWS Lambda se agregó soporte para este tiempo de ejecución.

Fecha del cambio	ID y título de control	Descripción del cambio
26 de marzo de 2025	[EKS.2] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible	Este control comprueba si un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) se ejecuta en una versión de Kubernetes compatible. Para el <code>oldestVersionSupported</code> parámetro, Security Hub CSPM cambió el valor de <code>a1.29.1.30</code> a <code>1.30</code>. La versión más antigua compatible de Kubernetes es ahora <code>1.30</code>.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de marzo de 2025	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos	Este control comprueba si la configuración del tiempo de ejecución de una AWS Lambda función coincide con los valores esperados para los tiempos de ejecución compatibles en cada idioma. El CSPM de Security Hub ya no admite dotnet6 ni python3.8 como valores de parámetro para este control. AWS Lambda ya no admite estos tiempos de ejecución.

Fecha del cambio	ID y título de control	Descripción del cambio
7 de marzo de 2025	Las instancias de RDS [RDS.18] deben implementarse en una VPC	Security Hub CSPM eliminó este control del estándar de mejores prácticas de seguridad AWS fundamentales y automatizó las comprobaciones de los requisitos del NIST SP 800-53 Rev. 5. Desde que se retiraron las redes Amazon EC2 - Classic, las instancias de Amazon Relational Database Service (Amazon RDS) ya no se pueden implementar fuera de una VPC. El control sigue formando parte del estándar de administración de servicios .AWS Control Tower
10 de enero de 2025	[Glue.2] Los trabajos de AWS pegado deberían tener habilitado el registro	Security Hub CSPM retiró este control y lo eliminó de todos los estándares.
20 de diciembre de 2024	EC26.1 a 1.69 EC2	Security Hub CSPM anuló la versión de los controles EC2 .61 a EC2 .169.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de diciembre de 2024	Las instancias RDS [RDS.23] no deben usar el puerto predeterminado de un motor de base de datos	El RDS.23 comprueba si un clúster o instancia de Amazon Relational Database Service (Amazon RDS) utiliza un puerto distinto del puerto predeterminado del motor de base de datos. Hemos actualizado el control para que la AWS Config regla subyacente devuelva un resultado de las instancias de NOT_APPLICABLE RDS que forman parte de un clúster.

Fecha del cambio	ID y título de control	Descripción del cambio
2 de diciembre de 2024	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos	Lambda.2 comprueba si la configuración de la AWS Lambda función para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. Security Hub CSPM ahora admite <code>nodejs22.x</code> como parámetro.
26 de noviembre de 2024	[EKS.2] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible	Este control comprueba si un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) se ejecuta en una versión de Kubernetes compatible. La versión compatible más antigua es ahora. 1.29

Fecha del cambio	ID y título de control	Descripción del cambio
20 de noviembre de 2024	[Config.1] AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos	La configuración 1 comprueba si AWS Config está habilitada, usa la función vinculada al servicio y registra los recursos para los controles habilitados. Security Hub CSPM aumentó la severidad de este control de aMEDIUM. CRITICAL Security Hub CSPM también agregó nuevos códigos de estado y motivos de estado para los hallazgos fallidos de Config.1. Estos cambios reflejan la importancia de la configuración 1 para el funcionamiento de los controles CSPM de Security Hub. Si tiene deshabilitado el registro de recursos AWS Config o el registro de recursos, es posible que reciba resultados de control inexactos.

Fecha del cambio	ID y título de control	Descripción del cambio
		Para recibir una PASSED búsqueda de Config.1, active el registro de recursos para los recursos que correspondan a los controles CSPM de Security Hub habilitados y deshabilite los controles que no sean necesarios en su organización. Para obtener instrucciones sobre la configuración AWS Config de Security Hub CSPM, consulte. Habilitación y configuración AWS Config de Security Hub CSPM Para obtener una lista de los controles CSPM de Security Hub y sus recursos correspondientes, consulte. AWS Config Recursos necesarios para los hallazgos de control

Fecha del cambio	ID y título de control	Descripción del cambio
12 de noviembre de 2024	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos	Lambda.2 comprueba si la configuración de la AWS Lambda función para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. Security Hub CSPM ahora admite python3.13 como parámetro.
11 de octubre de 2024	ElastiCache controles	Se han cambiado los títulos de los controles para las versiones ElastiCache 3.3, ElastiCache .4, ElastiCache .5 y ElastiCache .7. Los títulos ya no mencionan Redis OSS porque los controles también se aplican a Valkey. ElastiCache

Fecha del cambio	ID y título de control	Descripción del cambio
27 de septiembre de 2024	[ELB.4] El equilibrador de carga de aplicación debe configurarse para eliminar los encabezados http no válidos	Se cambió el título del control de El equilibrador de carga de aplicación debe configurarse para eliminar los encabezados http a El equilibrador de carga de aplicación debe configurarse para eliminar los encabezados http no válidos.
19 de agosto de 2024	El título cambia a DMS.12 y controles ElastiCache	Se han cambiado los títulos de los controles de los DMS.12 y ElastiCache de 1.1 a 0.7. ElastiCache Hemos cambiado estos títulos para reflejar un cambio de nombre en el servicio Amazon ElastiCache (Redis OSS).

Fecha del cambio	ID y título de control	Descripción del cambio
15 de agosto de 2024	[Config.1] AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos	La configuración 1 comprueba si AWS Config está habilitada, usa la función vinculada al servicio y registra los recursos para los controles habilitados. Security Hub CSPM agregó un parámetro de control personalizado denominado <code>includeConfigureServiceLinkedRoleCheck</code> . Si establece este parámetro en <code>false</code> , puede optar por no comprobar si AWS Config utiliza el rol vinculado al servicio.
31 de julio de 2024	Los perfiles de AWS IoT Device Defender seguridad [IoT.1] deben estar etiquetados	Se cambió el título del control de Los perfiles de seguridad de AWS IoT Core deben estar etiquetados a Los perfiles de seguridad de AWS IoT Device Defender deben estar etiquetados.

Fecha del cambio	ID y título de control	Descripción del cambio
29 de julio de 2024	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos	Lambda.2 comprueba si la configuración de la AWS Lambda función para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. Security Hub CSPM ya no admite <code>nodejs16.x</code> como parámetro.
29 de julio de 2024	[EKS.2] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible	Este control comprueba si un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) se ejecuta en una versión de Kubernetes compatible. La versión compatible más antigua es 1.28.

Fecha del cambio	ID y título de control	Descripción del cambio
25 de junio de 2024	[Config.1] AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos	Este control comprueba si AWS Config está habilitado o, usa el rol vinculado al servicio y registra los recursos de los controles habilitados. Security Hub CSPM actualizó el título del control para reflejar lo que evalúa el control.
14 de junio de 2024	[RDS.34] Los clústeres de bases de datos Aurora MySQL deberían publicar los registros de auditoría en Logs CloudWatch	Este control comprueba si un clúster de base de datos Amazon Aurora MySQL está configurado para publicar registros de auditoría en Amazon CloudWatch Logs. Security Hub CSPM actualizó el control para que no genere hallazgos para los clústeres de bases de datos Aurora Serverless v1.

Fecha del cambio	ID y título de control	Descripción del cambio
11 de junio de 2024	[EKS.2] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible	Este control comprueba si un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) se ejecuta en una versión de Kubernetes compatible. La versión compatible más antigua es 1.27.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de junio de 2024	[Config.1] AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos	Este control comprueba si AWS Config está activado y el registro de AWS Config recursos está activado. Anteriormente, el control solo generaba un resultado PASSED si se configuraba el registro para todos los recursos. Security Hub CSPM actualizó el control para PASSED detectar cuando la grabación está activada para los recursos necesarios para los controles habilitados. El control también se actualizó para comprobar si se utiliza el rol vinculado al servicio de AWS Config , que proporciona permisos para registrar los recursos necesarios.

Fecha del cambio	ID y título de control	Descripción del cambio
8 de mayo de 2024	[S3.20] Los buckets de uso general de S3 deben tener habilitada la eliminación de MFA	Este control comprueba si el bucket con control de versiones de uso general de Amazon S3 tiene habilitada la eliminación de la autenticación multifactor (MFA). Anteriormente, el control generaba un resultado FAILED para los buckets que tenían una configuración de ciclo de vida. Sin embargo, la eliminación de la MFA con el control de versiones no se puede habilitar en un bucket que tenga una configuración de ciclo de vida. Security Hub CSPM actualizó el control para no detectar ningún hallazgo en los buckets que tienen una configuración de ciclo de vida. La descripción del control se actualizó para

Fecha del cambio	ID y título de control	Descripción del cambio
		reflejar el comportamiento actual.
2 de mayo de 2024	[EKS.2] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible	Security Hub (CSPM) actualizó la versión compatible más antigua de Kubernetes en la que se puede ejecutar el clúster de Amazon EKS para obtener una conclusión válida. La versión compatible más antigua actual es Kubernetes 1.26.

Fecha del cambio	ID y título de control	Descripción del cambio
30 de abril de 2024	[CloudTrail.3] Al menos un CloudTrail registro de seguimiento debe habilitarse	Se ha cambiado el título del control de «CloudTrail Debe estar activado» a «Al menos una CloudTrail pista debe estar habilitada». Actualmente, este control produce un PASSED resultado si un sendero Cuenta de AWS tiene activado al menos un CloudTrail sendero. El título y la descripción se modificaron para reflejar con precisión el comportamiento actual.

Fecha del cambio	ID y título de control	Descripción del cambio
29 de abril de 2024	[AutoScaling.1] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar las comprobaciones de estado del ELB	Se cambió el título del control de Los grupos de escalado automático asociados a un equilibrador de carga clásico deben usar las comprobaciones de estado a Los grupos de escalado automático asociados a un equilibrador de carga deben usar comprobaciones de estado de ELB. Actualmente, este control evalúa los equilibradores de carga clásicos, de red, de puerta de enlace y de aplicaciones. El título y la descripción se modificaron para reflejar con precisión el comportamiento actual.

Fecha del cambio	ID y título de control	Descripción del cambio
19 de abril de 2024	[CloudTrail.1] CloudTrail debe habilitarse y configurarse con al menos un registro de seguimiento para varias regiones que incluya eventos de administración de lectura y escritura	El control comprueba si AWS CloudTrail está habilitado y configurado con al menos un registro multirregional que incluya eventos de administración de lectura y escritura . Anteriormente, el control generaba PASSED resultados de forma incorrecta cuando una cuenta tenía CloudTrail habilitada y configurada al menos un registro multirregional, incluso si ningún registro capturaba los eventos de administración de lectura y escritura . El control ahora genera un PASSED resultado solo cuando CloudTrail está habilitado y configurado con al menos un registro multirregional que captura los eventos de administr

Fecha del cambio	ID y título de control	Descripción del cambio
		ación de lectura y escritura.
10 de abril de 2024	[Athena.1] Los grupos de trabajo de Athena deben estar cifrados en reposo	Security Hub CSPM retiró este control y lo eliminó de todos los estándares. Los grupos de trabajo de Athena envían registros a buckets de Amazon Simple Storage Service (Amazon S3). Amazon S3 ahora ofrece cifrado predeterminado con claves administradas de S3 (SS3-S3) en buckets S3 nuevos y existentes.
10 de abril de 2024	[AutoScaling.4] La configuración de inicio de grupos de Auto Scaling no debe tener un límite de saltos de respuesta de metadatos superior a 1	Security Hub CSPM retiró este control y lo eliminó de todos los estándares. Los límites de saltos de respuesta de metadatos para las instancias de Amazon Elastic Compute Cloud (Amazon EC2) dependen de la carga de trabajo.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de abril de 2024	[CloudFormation.1] las CloudFormation pilas deben integrarse con el Simple Notification Service (SNS)	Security Hub CSPM retiró este control y lo eliminó de todos los estándares. Integrar AWS CloudFormation pilas con temas de Amazon SNS ya no es una práctica recomendada de seguridad. Si bien la integración de CloudFormation pilas importantes con los temas de SNS puede resultar útil, no es necesaria para todas las pilas.
10 de abril de 2024	[CodeBuild.5] Los entornos de CodeBuild proyectos no deberían tener habilitado el modo privilegiado	Security Hub CSPM retiró este control y lo eliminó de todos los estándares. Habilitar el modo privilegiado en un CodeBuild proyecto no supone un riesgo adicional para el entorno del cliente.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de abril de 2024	[IAM.20] Evitar el uso del usuario raíz	Security Hub CSPM retiró este control y lo eliminó de todos los estándares. El propósito de este control está cubierto por otro control, [CloudWatch.1] Debe existir un filtro de métricas de registro y una alarma para el uso del usuario «raíz» .
10 de abril de 2024	[SNS.2] Debe habilitarse el registro del estado de la entrega para los mensajes de notificación enviados a un tema	Security Hub CSPM retiró este control y lo eliminó de todos los estándares. Registrar el estado de entrega de los temas de SNS ya no es una práctica de seguridad recomendada. Aunque registrar el estado de entrega de los temas importantes del SNS puede resultar útil, no es obligatorio para todos los temas.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de abril de 2024	[S3.10] Los buckets de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida	Security Hub CSPM eliminó este control de AWS Foundational Security Best Practices y Service-Managed Standard: AWS Control Tower. El propósito de este control está cubierto por otros dos controles: [S3.13] Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida y [S3.14] Los buckets de uso general de S3 deben tener habilitado el control de versiones . Este control sigue siendo parte del NIST SP 800-53 Rev. 5.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de abril de 2024	[S3.11] Los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos	Security Hub CSPM eliminó este control de AWS Foundational Security Best Practices y Service-Managed Standard: AWS Control Tower. Si bien hay algunos casos en los que las notificaciones de eventos para los buckets de S3 son útiles, no se trata de una práctica de seguridad universal recomendada. Este control sigue siendo parte del NIST SP 800-53 Rev. 5.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de abril de 2024	[SNS.1] Los temas de SNS deben cifrarse en reposo mediante AWS KMS	Security Hub CSPM eliminó este control de AWS Foundatio nal Security Best Practices y Service-Managed Standard:. AWS Control Tower De forma predeterm inada, SNS cifra los temas en reposo mediante el cifrado de disco. Para más información, consulte Cifrado de datos . Ya no se recomienda AWS KMS su uso para cifrar temas como una mejor práctica de seguridad . Este control sigue siendo parte del NIST SP 800-53 Rev. 5.

Fecha del cambio	ID y título de control	Descripción del cambio
8 de abril de 2024	[ELB.6] La protección contra la eliminación de un equilibrador de carga de aplicación, de puerta de enlace y de red debe estar habilitada	Se cambió el título del control de El equilibrador de carga de aplicación debe tener habilitada la protección contra eliminaciones a Los equilibradores de carga de red, de las aplicaciones y de la puerta de enlace deben tener habilitada la protección contra eliminaciones. Actualmente, este control evalúa los equilibradores de carga de red, puertas de enlace y aplicaciones. El título y la descripción se modificaron para reflejar con precisión el comportamiento actual.

Fecha del cambio	ID y título de control	Descripción del cambio
22 de marzo de 2024	[Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente	Se cambió el título de control de Las conexiones a OpenSearch los dominios deben cifrarse mediante TLS 1.2 a Las conexiones a OpenSearch los dominios deben cifrarse mediante la última política de seguridad de TLS. Anteriormente, el control solo comprobaba si las conexiones a los OpenSearch dominios utilizaban TLS 1.2. El control ahora determina si los OpenSearch dominios están cifrados con la última política de seguridad de TLS. PASSED El título y la descripción del control se actualizaron para reflejar el comportamiento actual.

Fecha del cambio	ID y título de control	Descripción del cambio
22 de marzo de 2024	[ES.8] Las conexiones a dominios de Elasticsearch deben estar cifradas conforme a la política de seguridad TLS más reciente	Se cambió el título del control de Las conexiones a dominios de Elasticsearch deben estar cifradas a través de TLS 1.2 a Las conexiones a los dominios de Elasticsearch deben estar cifrados a través de la última política de seguridad de TLS. Anteriormente, el control solo comprobaba si las conexiones a los dominios de Elasticsearch utilizaban TLS 1.2. El control ahora genera un resultado PASSED si los dominios de Elasticsearch están cifrados a través de la última política de seguridad de TLS. El título y la descripción del control se actualizaron para reflejar el comportamiento actual.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.1] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público	El título cambió de La configuración del bloqueo de acceso público de S3 debe estar habilitada a Los buckets de uso general de S3 deben tener el bloqueo de acceso público habilitado. Security Hub CSPM cambió el título para dar cuenta de un nuevo tipo de bucket de S3.
12 de marzo de 2024	[S3.2] Los buckets de uso general de S3 deben bloquear el acceso público de lectura	Se cambió el título de Los buckets de S3 deben prohibir el acceso de lectura público a Los buckets de uso general de S3 deben bloquear el acceso de lectura público. Security Hub CSPM cambió el título para dar cuenta de un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.3] Los buckets de uso general de S3 deben bloquear el acceso público de escritura	Se cambió el título de Los buckets de S3 deben prohibir el acceso de escritura público a Los buckets de uso general de S3 deben bloquear el acceso de escritura público. Security Hub CSPM cambió el título para dar cuenta de un nuevo tipo de bucket de S3.
12 de marzo de 2024	[S3.5] En las solicitudes de los buckets de uso general de S3, se debe pedir el uso de SSL	Se cambió el título de Los buckets de S3 deben requerir solicitudes para usar Secure Socket Layer a Los buckets de uso general de S3 deben requerir solicitud es para usar SSL. Security Hub CSPM cambió el título para dar cuenta de un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.6] Las políticas de compartimentos de uso general de S3 deberían restringir el acceso a otros Cuentas de AWS	Si se ha cambiado el título de S3, los permisos concedidos a otras Cuentas de AWS políticas de bucket deberían restringirse a las políticas de bucket de uso general de S3. Las políticas de bucket de uso general deberían restringir el acceso a otras políticas. Cuentas de AWS Security Hub CSPM cambió el título para dar cuenta de un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.7] Los buckets de uso general de S3 deben usar la replicación entre regiones	Se cambió el título de Los buckets de S3 deben tener la replicación entre regiones habilitada a Los buckets de uso general de S3 deben usar la replicación entre regiones. Security Hub CSPM cambió el título para dar cuenta de un nuevo tipo de bucket de S3.
12 de marzo de 2024	[S3.7] Los buckets de uso general de S3 deben usar la replicación entre regiones	Se cambió el título de Los buckets de S3 deben tener la replicación entre regiones habilitada a Los buckets de uso general de S3 deben usar la replicación entre regiones. Security Hub CSPM cambió el título para dar cuenta de un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.8] Los buckets de uso general de S3 deben bloquear el acceso público	Se cambió el título de La configuración de acceso público al bloque S3 debe estar habilitada en el nivel de bucket a Los buckets de uso general de S3 deben bloquear el acceso público. Security Hub CSPM cambió el título para dar cuenta de un nuevo tipo de bucket de S3.
12 de marzo de 2024	[S3.9] Los buckets de uso general de S3 deben tener habilitado el registro de acceso al servidor	Se cambió el título de Se debe habilitar el registro de acceso al bucket de S3 a Se debe habilitar el registro de acceso al servidor para los buckets de uso general de S3. Security Hub CSPM cambió el título para dar cuenta de un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.10] Los buckets de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida	Se cambió el título de Los buckets de S3 con el control de versiones habilitado deben tener configuradas las políticas de ciclo de vida a Los buckets de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida. Security Hub CSPM cambió el título para dar cuenta de un nuevo tipo de bucket de S3.
12 de marzo de 2024	[S3.11] Los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos	Se cambió el título de Los buckets de S3 deben tener las notificaciones de eventos habilitadas a Los buckets de uso general de S3 deben tener las notificaciones de eventos habilitadas. Security Hub CSPM cambió el título para dar cuenta de un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.12] no ACLs debe usarse para administrar el acceso de los usuarios a los depósitos de uso general de S3	El nombre cambiado de las listas de control de acceso de S3 (ACLs) no debe usarse para administrar el acceso de los usuarios a los buckets a no ACLs debe usarse para administrar el acceso de los usuarios a los buckets de uso general de S3. Security Hub CSPM cambió el título para dar cuenta de un nuevo tipo de bucket de S3.
12 de marzo de 2024	[S3.13] Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida	Se cambió el título de Los buckets de S3 deben tener configuradas las políticas de ciclo de vida a Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida. Security Hub CSPM cambió el título para dar cuenta de un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.14] Los buckets de uso general de S3 deben tener habilitado el control de versiones	Se cambió el título de Los buckets de S3 deben utilizar el control de versiones a Los buckets de uso general de S3 deben tener el control de versiones habilitado. Security Hub CSPM cambió el título para dar cuenta de un nuevo tipo de bucket de S3.
12 de marzo de 2024	[S3.15] Los buckets de uso general de S3 deben tener habilitado el bloqueo de objetos	Se cambió el título de Los buckets de S3 deben configurarse para usar el Bloqueo de objetos a Los buckets de uso general de S3 deben tener Bloqueo de objetos habilitado. Security Hub CSPM cambió el título para dar cuenta de un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
12 de marzo de 2024	[S3.17] Los depósitos de uso general de S3 deben cifrarse en reposo con AWS KMS keys	Se cambió el título de Los buckets de S3 deben estar cifrados en reposo a través de AWS KMS keys a Los buckets de uso general de S3 deben estar cifrados en reposo a través de AWS KMS keys. Security Hub CSPM cambió el título para dar cuenta de un nuevo tipo de bucket de S3.
7 de marzo de 2024	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos	Lambda.2 comprueba si la configuración de la AWS Lambda función para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. Security Hub CSPM ahora admite node.js20.x y ruby3.3 como parámetros.

Fecha del cambio	ID y título de control	Descripción del cambio
22 de febrero de 2024	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos	Lambda.2 comprueba si la configuración de la AWS Lambda función para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. Security Hub CSPM ahora admite dotnet8 como parámetro.
5 de febrero de 2024	[EKS.2] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible	Security Hub (CSPM) actualizó la versión compatible más antigua de Kubernetes en la que se puede ejecutar el clúster de Amazon EKS para obtener una conclusión válida. La versión compatible más antigua actual es Kubernetes 1.25.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de enero de 2024	[CodeBuild.1] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales	El título modificado o del repositorio fuente de Bitbucket CodeBuild GitHub o el que URLs debe utilizarse OAuth en el repositorio fuente de CodeBuild Bitbucket no debe contener credenciales confidenciales. URLs Security Hub CSPM eliminó la mención OAuth porque otros métodos de conexión también pueden ser seguros. CSPM eliminó la mención de Security Hub GitHub porque ya no es posible tener un token de acceso personal o un nombre de usuario y contraseña en el repositorio de GitHub origen. URLs

Fecha del cambio	ID y título de control	Descripción del cambio
8 de enero de 2024	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos	Lambda.2 comprueba si la configuración de la AWS Lambda función para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. El CSPM de Security Hub ya no admite go1.x ni java8 como parámetros porque se trata de tiempos de ejecución retirados.

Fecha del cambio	ID y título de control	Descripción del cambio
29 de diciembre de 2023	Las instancias de base de datos de RDS [RDS.8] deben tener habilitada la protección contra la eliminación	RDS.8 comprueba si una instancia de base de datos de Amazon RDS que utiliza uno de los motores de bases de datos compatibles tiene habilitada la protección contra eliminaciones. Security Hub CSPM ahora admite y <code>oracle-se2-cdb</code> como <code>custom-oracle-ee</code> motores <code>oracle-ee-cdb</code> de bases de datos.

Fecha del cambio	ID y título de control	Descripción del cambio
22 de diciembre de 2023	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos	Lambda.2 comprueba si la configuración de la AWS Lambda función para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. Security Hub CSPM ahora admite java21 y python3.12 como parámetros. Security Hub CSPM ya no admite ruby2.7 como parámetro.

Fecha del cambio	ID y título de control	Descripción del cambio
15 de diciembre de 2023	[CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado	CloudFront.1 comprueba si una CloudFront distribución de Amazon tiene configurado un objeto raíz predeterminado. Security Hub CSPM redujo la severidad de este control de CRITICAL a HIGH porque se recomienda a agregar el objeto raíz predeterminado y depende de la aplicación del usuario y de los requisitos específicos.
5 de diciembre de 2023	[EC2.13] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 o: :/0 al puerto 22	Se ha cambiado el título del control de Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 al puerto 22 a Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 o ::/0 al puerto 22.

Fecha del cambio	ID y título de control	Descripción del cambio
5 de diciembre de 2023	[EC2.14] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 o: :/0 al puerto 3389	Se ha cambiado el título del control de Asegúrese de que ningún grupo de seguridad permita la entrada desde 0.0.0.0/0 al puerto 3389 a Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 o ::/0 al puerto 3389.

Fecha del cambio	ID y título de control	Descripción del cambio
5 de diciembre de 2023	[RDS.9] Las instancias de base de datos de RDS deben publicar los registros en Logs CloudWatch	Se ha cambiado el título del control: el registro de bases de datos debe estar activado y las instancias de base de datos de RDS deben publicar los registros en los registros. CloudWatch Security Hub CSPM identificó que este control solo comprueba si los registros se publican en Amazon CloudWatch Logs y no comprueba si los registros de RDS están habilitados. El control determina si las instancias de PASSED base de datos de RDS están configuradas para publicar registros en Logs. CloudWatch El título del control se ha actualizado para reflejar el comportamiento actual.

Fecha del cambio	ID y título de control	Descripción del cambio
5 de diciembre de 2023	[EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría	Este control comprueba si los clústeres de Amazon EKS tienen habilitado el registro de auditoría . La AWS Config regla que utiliza Security Hub CSPM para evaluar este control cambió de eks-cluster-logging-enabled a eks-cluster-log-enabled

Fecha del cambio	ID y título de control	Descripción del cambio
17 de noviembre de 2023	[EC219] Los grupos de seguridad no deben permitir el acceso irrestricto a los puertos de alto riesgo	EC2.19 comprueba si el tráfico entrante sin restricciones de un grupo de seguridad es accesible desde los puertos especificados que se consideran de alto riesgo. Security Hub CSPM actualizó este control para tener en cuenta las listas de prefijos administradas cuando se proporcionan como origen de una regla de grupo de seguridad. El control genera un resultado FAILED si las listas de prefijos contienen las cadenas "0.0.0.0/0" o "::/0".

Fecha del cambio	ID y título de control	Descripción del cambio
16 de noviembre de 2023	[CloudWatch.15] CloudWatch las alarmas deben tener configuradas acciones específicas	Al cambiar el título del control, CloudWatch las alarmas deberían tener una acción configurada para el estado de ALARMA a CloudWatch las alarmas deberían tener configuradas acciones específicas.
16 de noviembre de 2023	[CloudWatch.16] Los grupos de CloudWatch registros deben retenerse durante un periodo específico	El título de control modificado, de grupos de CloudWatch registros, debe conservarse durante al menos 1 año, a grupos de CloudWatch registros, debe conservarse durante un período de tiempo específico.

Fecha del cambio	ID y título de control	Descripción del cambio
16 de noviembre de 2023	[Lambda.5] Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad	Se ha cambiado el título de control de Las funciones de Lambda de la VPC deben funcionar en más de una zona de disponibilidad a Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad.
16 de noviembre de 2023	[AppSync.2] AWS AppSync debe tener habilitado el registro a nivel de campo	Se ha cambiado el título de control de AWS AppSync debe tener activado el registro a nivel de solicitud y a nivel de campo a AWS AppSync debe tener habilitado el registro a nivel de campo.

Fecha del cambio	ID y título de control	Descripción del cambio
16 de noviembre de 2023	[EMR.1] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas	Se cambió el título de control de los nodos maestros del MapReduce clúster de Amazon Elastic no deberían tener direcciones IP públicas a los nodos principales del clúster de Amazon EMR no deberían tener direcciones IP públicas.
16 de noviembre de 2023	Los OpenSearch dominios [Opensearch.2] no deben ser de acceso público	El título de control modificado de OpenSearch los dominios debería estar en una VPC a OpenSearchdominios que no deberían ser de acceso público.
16 de noviembre de 2023	[ES.2] Los dominios de Elasticsearch no deben ser de acceso público	Se ha cambiado el título de control de Los dominios de Elasticsearch deben estar en una VPC a Los dominios de Elasticsearch no deben ser de acceso público.

Fecha del cambio	ID y título de control	Descripción del cambio
31 de octubre de 2023	[ES.4] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros	ES.4 comprueba si los dominios de Elasticsearch están configurados para enviar registros de errores a Amazon Logs. CloudWatch Anteriormente, el control PASSED encontró un dominio de Elasticsearch que tenía todos los registros configurados para enviarlos a Logs. CloudWatch Security Hub CSPM actualizó el control para producir una PASSED búsqueda solo para un dominio de Elasticsearch que esté configurado para enviar registros de errores a Logs. CloudWatch El control también se actualizó para excluir de la evaluación versiones de Elasticsearch que no admiten registros de errores.

Fecha del cambio	ID y título de control	Descripción del cambio
16 de octubre de 2023	[EC2.13] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 o ::/0 al puerto 22	EC2La versión .13 comprueba si los grupos de seguridad permiten el acceso sin restricciones al puerto 22. Security Hub CSPM actualizó este control para tener en cuenta las listas de prefijos administradas cuando se proporcionan como origen de una regla de grupo de seguridad. El control genera un resultado FAILED si las listas de prefijos contienen las cadenas "0.0.0.0/0" o "::/0".

Fecha del cambio	ID y título de control	Descripción del cambio
16 de octubre de 2023	[EC2.14] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 o ::/0 al puerto 3389	EC2.14 comprueba si los grupos de seguridad permiten el acceso sin restricciones al puerto 3389. Security Hub CSPM actualizó este control para tener en cuenta las listas de prefijos administradas cuando se proporcionan como origen de una regla de grupo de seguridad. El control genera un resultado FAILED si las listas de prefijos contienen las cadenas "0.0.0.0/0" o "::/0".

Fecha del cambio	ID y título de control	Descripción del cambio
16 de octubre de 2023	[EC2.18] Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados	EC2.18 comprueba si los grupos de seguridad que se utilizan permiten el tráfico entrante sin restricciones. Security Hub CSPM actualizó este control para tener en cuenta las listas de prefijos administradas cuando se proporcionan como origen de una regla de grupo de seguridad. El control genera un resultado FAILED si las listas de prefijos contienen las cadenas "0.0.0.0/0" o "::/0".

Fecha del cambio	ID y título de control	Descripción del cambio
16 de octubre de 2023	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos	Lambda.2 comprueba si la configuración de la AWS Lambda función para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. Security Hub CSPM ahora admite python3.11 como parámetro.
4 de octubre de 2023	[S3.7] Los buckets de uso general de S3 deben usar la replicación entre regiones	Security Hub CSPM agregó el parámetro ReplicationType con un valor de CROSS-REGION para garantizar que los buckets de S3 tengan habilitada la replicación entre regiones en lugar de la replicación en la misma región.

Fecha del cambio	ID y título de control	Descripción del cambio
27 de septiembre de 2023	[EKS.2] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible	Security Hub (CSPM) actualizó la versión compatible más antigua de Kubernetes en la que se puede ejecutar el clúster de Amazon EKS para obtener una conclusión válida. La versión compatible más antigua actual es Kubernetes 1.24.
20 de septiembre de 2023	[CloudFront.2] las CloudFront distribuciones deben tener habilitada la identidad de acceso de origen	Security Hub CSPM retiró este control y lo eliminó de todos los estándares. En su lugar, consulte [CloudFront.13] CloudFront Las distribuciones deben usar el control de acceso de origen . El control de acceso de Origen es la mejor práctica de seguridad actual. Este control se eliminará de la documentación en 90 días.

Fecha del cambio	ID y título de control	Descripción del cambio
20 de septiembre de 2023	[EC2.22] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse	Security Hub CSPM eliminó este control de AWS Foundational Security Best Practices (FSBP) y del National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5. Sigue formando parte del estándar de gestión de servicios: AWS Control Tower Este control produce una comprobación válida si los grupos de seguridad están conectados a EC2 instancias o a una interface de red elástica. Sin embargo, en algunos casos de uso, los grupos de seguridad independientes no representan un riesgo para la seguridad. Puede usar otros EC2 controles, como EC2 .2, EC2 .13, EC2 .14, EC2 .18 y EC2 .19, para

Fecha del cambio	ID y título de control	Descripción del cambio
		monitorear sus grupos de seguridad.
20 de septiembre de 2023	[EC2.29] EC2 las instancias deben lanzarse en una VPC	Security Hub CSPM retiró este control y lo eliminó de todos los estándares. Amazon EC2 ha migrado las instancias clásicas a una VPC. Este control se eliminará de la documentación en 90 días.

Fecha del cambio	ID y título de control	Descripción del cambio
20 de septiembre de 2023	[S3.4] Los buckets de S3 deben tener habilitado el cifrado del servidor	Security Hub CSPM retiró este control y lo eliminó de todos los estándares. Amazon S3 ahora ofrece cifrado predeterminado con claves administradas de S3 (SS3-S3) en buckets S3 nuevos y existentes. La configuración de cifrado no ha cambiado para los buckets existentes que se cifran con el cifrado SS3 -S3 o SS3 -KMS del lado del servidor. Este control se eliminará de la documentación en 90 días.

Fecha del cambio	ID y título de control	Descripción del cambio
14 de septiembre de 2023	[EC22] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente	Se cambió el título de control de El grupo de seguridad predeterminado de VPC no debe permitir el tráfico entrante ni saliente a Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente.
14 de septiembre de 2023	[IAM.9] La MFA debe estar habilitada para el usuario raíz	Se cambió el título de control de La MFA virtual debe estar habilitada para el usuario raíz a La MFA debe estar habilitada para el usuario raíz.

Fecha del cambio	ID y título de control	Descripción del cambio
14 de septiembre de 2023	<u>Las suscripciones de notificación de eventos de RDS [RDS.19] existentes deben configurarse para los eventos de clúster críticos</u>	Se cambió el título de control de Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos de clúster críticos a Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos de clúster críticos.
14 de septiembre de 2023	<u>Las suscripciones de notificación de eventos de RDS [RDS.20] existentes deben configurarse para eventos críticos de instancias de bases de datos</u>	Se cambió el título de control de Se debe configurar una suscripción a las notificaciones de eventos de RDS para los eventos críticos de instancias de bases de datos a Las suscripciones de notificación de eventos de RDS existentes deben configurarse para los eventos críticos de instancias de bases de datos.

Fecha del cambio	ID y título de control	Descripción del cambio
14 de septiembre de 2023	Las reglas de [WAF.2] Regionales AWS WAF clásicas deben tener al menos una condición	Se cambió el título de control de Una regla regional de WAF debe tener al menos una condición a Las reglas regionales de AWS WAF Classic deben tener al menos una condición.
14 de septiembre de 2023	Los grupos de reglas de [WAF.3] Regionales AWS WAF clásicos deben tener al menos una regla	Se cambió el título de control de Un grupo de reglas regionales de WAF debe tener al menos una regla a Los grupos de reglas regionales de AWS WAF Classic deben tener al menos una regla.
14 de septiembre de 2023	La web de [WAF.4] Regionales AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas	Se ha cambiado el título del control: Una ACL web regional de WAF debe tener al menos una regla o grupo de reglas a una web regional AWS WAF clásica, ACLs debe tener al menos una regla o grupo de reglas.

Fecha del cambio	ID y título de control	Descripción del cambio
14 de septiembre de 2023	Las reglas globales de [WAF.6] AWS WAF clásicas deben tener al menos una condición	Se cambió el título de control de Una regla global de WAF debe tener al menos una condición a Las reglas globales de AWS WAF Classic deben tener al menos una condición.
14 de septiembre de 2023	Los grupos de reglas globales de [WAF.7] AWS WAF clásicos deben tener al menos una regla	Se cambió el título de control de Un grupo de reglas globales de WAF debe tener al menos una regla a Los grupos de reglas globales de AWS WAF Classic deben tener al menos una regla.
14 de septiembre de 2023	La web de [WAF.8] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas	Se ha cambiado el título del control de una ACL web global de WAF que debe tener al menos una regla o grupo de reglas a una web global AWS WAF clásica que ACLs debe tener al menos una regla o grupo de reglas.

Fecha del cambio	ID y título de control	Descripción del cambio
14 de septiembre de 2023	La AWS WAF web de [WAF.10] ACLs debe tener al menos una regla o grupo de reglas	El título de control cambiado de una ACL WAFv2 web debe tener al menos una regla o grupo de reglas a AWS WAF web ACLs debe tener al menos una regla o grupo de reglas.
14 de septiembre de 2023	El registro de ACL AWS WAF web de [WAF.11] debe estar habilitado	Se cambió el título de control de El registro de la ACL web de AWS WAF v2 debe estar activado a El registro de la ACL web de AWS WAF debe estar habilitado.

Fecha del cambio	ID y título de control	Descripción del cambio
20 de julio de 2023	[S3.4] Los buckets de S3 deben tener habilitado o el cifrado del servidor	S3.4 comprueba si el bucket de Amazon S3 tiene habilitado el cifrado del lado del servidor o que la política de bucket de S3 deniega explícitamente las solicitudes PutObject sin cifrado del lado del servidor. Security Hub CSPM actualizó este control para incluir el cifrado de doble capa del lado del servidor con claves KMS (DSSE-KMS). El control genera un resultado aprobado cuando un bucket de S3 está cifrado con SSE-S3, SSE-KMS o DSSE-KMS.

Fecha del cambio	ID y título de control	Descripción del cambio
17 de julio de 2023	[S3.17] Los depósitos de uso general de S3 deben cifrarse en reposo con AWS KMS keys	S3.17 comprueba si un bucket de Amazon S3 está cifrado con un AWS KMS key. Security Hub CSPM actualizó este control para incluir el cifrado de doble capa del lado del servidor con claves KMS (DSSE-KMS). El control genera un resultado aprobado cuando un bucket de S3 está cifrado con SSE-KMS o DSSE-KMS.
9 de junio de 2023	[EKS.2] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible	EKS.2 comprueba si un clúster de Amazon EKS se está ejecutando en una versión compatible de Kubernetes. La versión compatible más antigua es ahora 1.23.

Fecha del cambio	ID y título de control	Descripción del cambio
9 de junio de 2023	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos	Lambda.2 comprueba si la configuración de la AWS Lambda función para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. Security Hub CSPM ahora admite ruby3.2 como parámetro.
5 de junio de 2023	[APIGateway.5] Los datos de la caché de la API de REST de API Gateway deben cifrarse en reposo	APIGateway.5. Comprueba si todos los métodos de las etapas de la API REST de Amazon API Gateway están cifrados en reposo. Security Hub CSPM actualizó el control para evaluar el cifrado de un método en particular solo cuando el almacenamiento en caché está habilitado para ese método.

Fecha del cambio	ID y título de control	Descripción del cambio
18 de mayo de 2023	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos	Lambda.2 comprueba si la configuración de la AWS Lambda función para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. Security Hub CSPM ahora admite java17 como parámetro.
18 de mayo de 2023	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos	Lambda.2 comprueba si la configuración de la AWS Lambda función para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. Security Hub CSPM ya no admite nodejs12.x como parámetro.

Fecha del cambio	ID y título de control	Descripción del cambio
23 de abril de 2023	[ECS.10] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate	ECS.10 comprueba si los servicios Fargate de Amazon ECS ejecutan la versión de la plataforma Fargate más reciente. Los clientes pueden implementar Amazon ECS a través de ECS directamente o mediante CodeDeploy. Security Hub CSPM actualizó este control para generar resultados aprobados cuando se utilizan CodeDeploy para implementar los servicios Fargate de ECS.

Fecha del cambio	ID y título de control	Descripción del cambio
20 de abril de 2023	[S3.6] Las políticas de compartimentos de uso general de S3 deberían restringir el acceso a otros Cuentas de AWS	El S3.6 comprueba si una política de bucket de Amazon Simple Storage Service (Amazon S3) impide que los directores de Cuentas de AWS otras entidades realicen acciones denegadas en los recursos del bucket de S3. Security Hub CSPM actualizó el control para tener en cuenta los condicionales de una política de bucket.
18 de abril de 2023	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos	Lambda.2 comprueba si la configuración de la AWS Lambda función para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. Security Hub CSPM ahora admite python3.10 como parámetro.

Fecha del cambio	ID y título de control	Descripción del cambio
18 de abril de 2023	[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos	Lambda.2 comprueba si la configuración de la AWS Lambda función para los tiempos de ejecución coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. Security Hub CSPM ya no admite dotnetcore3.1 como parámetro.

Fecha del cambio	ID y título de control	Descripción del cambio
17 de abril de 2023	Las instancias RDS [RDS.11] deben tener habilitadas las copias de seguridad automáticas	RDS.11 comprueba si las instancias de Amazon RDS tienen habilitada las copias de seguridad automáticas, con un periodo de retención de las copias de seguridad superior o igual a siete días. Security Hub CSPM actualizó este control para excluir las réplicas de lectura de la evaluación, ya que no todos los motores admiten copias de seguridad automatizadas en las réplicas de lectura. Además, RDS no ofrece la opción de especificar un periodo de retención de las copias de seguridad al crear réplicas de lectura. Las réplicas de lectura se crean con un periodo de retención predeterminado de la copia de seguridad de 0.

Controles de Security Hub para Cuentas de AWS

Estos controles de Security Hub evalúan Cuentas de AWS.

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Cuenta.1] La información de contacto de seguridad debe proporcionarse para un Cuenta de AWS

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

Categoría: Identificar > Configuración de recursos

Gravedad: media

Tipo de recurso: AWS:::Account

Regla de AWS Config : [security-account-information-provided](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si una cuenta de Amazon Web Services (AWS) tiene información de contacto de seguridad. El control falla si no se proporciona la información de contacto de seguridad de la cuenta.

Los contactos de seguridad alternativos te permiten AWS ponerte en contacto con otra persona en caso de que no estés disponible para resolver problemas relacionados con tu cuenta. Las notificaciones pueden provenir de Soporte otros equipos o de otros Servicio de AWS equipos sobre temas relacionados con la seguridad relacionados con tu Cuenta de AWS uso.

Corrección

Para añadir un contacto alternativo como contacto de seguridad al tuyo Cuenta de AWS, consulta [Actualizar tus contactos alternativos Cuenta de AWS en la Guía](#) de referencia de administración de AWS cuentas.

[Account.2] Cuentas de AWS debe formar parte de una organización AWS Organizations

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Gravedad: alta

Tipo de recurso: AWS:::Account

Regla de AWS Config : [account-part-of-organizations](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si una Cuenta de AWS forma parte de una organización gestionada a través de ella. AWS Organizations El control falla si la cuenta no forma parte de una organización.

Organizations le ayuda a administrar su entorno de forma centralizada a medida que amplía sus cargas de trabajo. AWS Puede usar varias Cuentas de AWS para aislar las cargas de trabajo que tienen requisitos de seguridad específicos o para cumplir con marcos como la HIPAA o la PCI. Al crear una organización, puede administrar varias cuentas como una sola unidad y administrar de forma centralizada su acceso a Servicios de AWS los recursos y las regiones.

Corrección

Para crear una nueva organización y Cuentas de AWS añadirla automáticamente, consulte [Creación de una organización](#) en la Guía del AWS Organizations usuario. Para añadir cuentas a una organización existente, consulte [Invitar a un usuario Cuenta de AWS a unirse a su organización](#) en la Guía del AWS Organizations usuario.

Controles de Security Hub para AWS Amplify

Estos controles de Security Hub evalúan el AWS Amplify servicio y los recursos. Es posible que los controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Amplify.1] Las aplicaciones de Amplify deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Amplify::App

Regla de AWS Config : [amplify-app-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Una lista de claves de etiquetas que no están en el sistema y que se deben asignar a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una AWS Amplify aplicación tiene las claves de etiqueta especificadas en el `requiredKeyTags` parámetro. El control falla si la aplicación no tiene ninguna clave de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no especificas ningún valor para el `requiredKeyTags` parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si la aplicación no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws :` prefijo.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarle a identificar, organizar, buscar y filtrar los recursos. También pueden ayudarte a realizar un seguimiento de las acciones y notificaciones de los propietarios de los recursos. También puedes usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas](#).

Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están pensadas para usarse con datos privados o confidenciales.

Corrección

Para obtener información sobre cómo añadir etiquetas a una AWS Amplify aplicación, consulta la [compatibilidad con el etiquetado de recursos](#) en la Guía del usuario de AWS Amplify hosting.

[Amplify.2] Las ramas de Amplify deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Amplify::Branch

Regla de AWS Config : [amplify-branch-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Una lista de claves de etiquetas no relacionadas con el sistema que se deben asignar a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una AWS Amplify rama tiene las claves de etiqueta especificadas en el `requiredKeyTags` parámetro. El control falla si la rama no tiene ninguna clave de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no especifica ningún valor para el `requiredKeyTags` parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si la rama no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws:` prefijo.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarle a identificar, organizar, buscar y filtrar los recursos. También pueden ayudarte a realizar un seguimiento de las acciones y notificaciones de los propietarios de los recursos. También puedes usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas](#).

Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están pensadas para usarse con datos privados o confidenciales.

Corrección

Para obtener información sobre cómo añadir etiquetas a una AWS Amplify sucursal, consulta la [compatibilidad con el etiquetado de recursos](#) en la Guía del usuario de AWS Amplify hosting.

Controles de Security Hub para Amazon API Gateway

Estos AWS Security Hub controles evalúan el servicio Amazon API Gateway y sus recursos. Es posible que los controles de no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[APIGateway.1] El registro de ejecución de WebSocket REST y API de API Gateway debe estar habilitado

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::ApiGateway::Stage, AWS::ApiGatewayV2::Stage

Regla de AWS Config : [api-gw-execution-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
loggingLevel	Nivel de registro	Enum	ERROR, INFO	No default value

Este control comprueba si todas las etapas de REST de Amazon API Gateway o API de Amazon WebSocket API Gateway tienen habilitado el registro. Se produce un error en el control si loggingLevel no figura como ERROR o INFO en todas las etapas de la API. A menos que se proporcionen valores personalizados de parámetros para indicar que se debe habilitar un tipo de registro específico, Security Hub genera un resultado válido si el nivel de registro es ERROR o INFO.

Las etapas API o REST de WebSocket API Gateway deben tener habilitados los registros relevantes. El registro de ejecución de WebSocket REST y API de API Gateway proporciona registros detallados de las solicitudes realizadas a las etapas de REST y WebSocket API de API Gateway. Las etapas incluyen las respuestas de backend de integración de API, las respuestas del autorizador de Lambda y los puntos de conexión requestId de AWS integración.

Corrección

Para habilitar el registro de las operaciones de WebSocket REST y API, consulte [Configurar el registro de CloudWatch API mediante la consola de API Gateway](#) en la Guía para desarrolladores de API Gateway.

[APIGateway.2] Las etapas de la API de REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3 (3), NIST.800-53.r5 SC-1 (4), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 Nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), Nist.800-171.r2 3.13.15

Categoría: Protección > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::ApiGateway::Stage

Regla de AWS Config : [api-gw-ssl-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las etapas de la API de REST de Amazon API Gateway tienen certificados SSL configurados. Los sistemas de backend utilizan estos certificados para autenticar que las solicitudes entrantes provienen de API Gateway.

Las etapas de la API de REST de API Gateway deben configurarse con certificados SSL para permitir que los sistemas de backend autenticuen que las solicitudes se originan en API Gateway.

Corrección

Para obtener instrucciones detalladas sobre cómo generar y configurar los certificados SSL de la API de REST de API Gateway, consulte [Generar y configurar un certificado SSL para la autenticación de backend](#) en la Guía para desarrolladores de API Gateway.

[APIGateway.3] Las etapas de la API de REST de API Gateway tener AWS X-Ray habilitado el rastreo

Requisitos relacionados: NIST.800-53.r5 CA-7

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::ApiGateway::Stage

Regla de AWS Config : [api-gw-xray-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el rastreo de AWS X-Ray activo está habilitado para las etapas de la API de REST de Amazon API Gateway.

El rastreo activo de X-Ray permite una respuesta más rápida a los cambios de rendimiento en la infraestructura subyacente. Los cambios en el rendimiento podrían provocar una falta de disponibilidad de la API. El rastreo activo de X-Ray proporciona métricas en tiempo real de las solicitudes de los usuarios que fluyen a través de las operaciones de la API de REST y los servicios conectados de API Gateway.

Corrección

Para obtener instrucciones detalladas sobre cómo habilitar el rastreo activo de X-Ray para las operaciones de la API de REST de API Gateway, consulte la [Compatibilidad con el rastreo activo de Amazon API Gateway para AWS X-Ray](#) en la Guía para desarrolladores de AWS X-Ray .

[APIGateway.4] La API Gateway debe estar asociada a una ACL web de WAF

Requisitos relacionados: NIST.800-53.r5 AC-4 (21)

Categoría: Proteger > Servicios de protección

Gravedad: media

Tipo de recurso: AWS::ApiGateway::Stage

Regla de AWS Config : [api-gw-associated-with-waf](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una etapa de API Gateway utiliza una lista de control de acceso (ACL) AWS WAF web de. Este control falla si una ACL AWS WAF web de no está conectada a una etapa REST de API Gateway.

AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones web APIs de ataques. Le permite configurar una web ACL, que son un conjunto de reglas que permiten, bloquean o cuentan solicitudes web en función de las reglas y condiciones de seguridad web personalizables que defina. Asegúrese de que la etapa de API Gateway esté asociada a una ACL AWS WAF web de para protegerla de ataques maliciosos.

Corrección

Para obtener información sobre cómo utilizar la consola de API Gateway para asociar una ACL web de AWS WAF Regional a una etapa de la API de API de API de API Gateway existente, consulte [AWS WAF Utilización para protegerla APIs](#) en la Guía para desarrolladores de API Gateway.

[APIGateway.5] Los datos de la caché de la API de REST de API Gateway deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger - Protección de datos - Cifrado de datos en reposo

Gravedad: media

Tipo de recurso: AWS::ApiGateway::Stage

Regla de AWS Config : api-gw-cache-encrypted (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si todos los métodos de las etapas de la API de REST de API Gateway que tienen la caché habilitada están cifrados. El control falla si algún método de una etapa de API de REST de API Gateway está configurado para almacenar en caché y la caché no está cifrada. Security Hub evalúa el cifrado de un método en particular solo cuando el almacenamiento en caché está habilitado para ese método.

El cifrado de los datos en reposo reduce el riesgo de que un usuario no autenticado acceda a los datos almacenados en el disco. AWS Añade otro conjunto de controles de acceso para limitar la capacidad de los usuarios no autorizados de acceder a los datos. Por ejemplo, se requieren permisos de API para descifrar los datos antes de que puedan leerse.

Las cachés de la API de REST de API Gateway deben cifrarse en reposo para ofrecer una capa de seguridad adicional.

Corrección

Para configurar el almacenamiento en caché de API para una etapa, consulte [Habilitar el almacenamiento en caché de Amazon API Gateway](#) en la Guía para desarrolladores de API Gateway. En Configuración de caché, seleccione Cifrar datos de caché.

[APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización

Requisitos relacionados: NIST.800-53.r5 CM-2 NIST.800-53.r5 AC-3, NIST.800-53.r5 CM-2 (2)

Categoría: Proteger > Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS::ApiGatewayV2::Route

Regla de AWS Config : [api-gwv2-authorization-type-configured](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
authorizationType	Tipo de autorización de las rutas de API	Enum	AWS_IAM, CUSTOM, JWT	Sin valor predeterminado

Este control comprueba si las rutas de Amazon API Gateway tienen un tipo de autorización. Se produce un error en el control si la ruta de API Gateway no tiene ningún tipo de autorización.

También, puede proporcionar un valor personalizado de parámetro si quiere que el control pase únicamente si la ruta utiliza el tipo de autorización especificado en el parámetro `authorizationType`.

API Gateway admite varios mecanismos para controlar y administrar el acceso a la API. Al especificar un tipo de autorización, puede restringir el acceso a tu API solo a los usuarios o procesos autorizados.

Corrección

Para establecer un tipo de autorización para HTTP APIs, consulte [Controlar y administrar el acceso a una API HTTP en API Gateway](#) en la Guía para desarrolladores de API Gateway. Para establecer un tipo de autorización para WebSocket APIs, consulte [Controlar y administrar el acceso a una WebSocket API en API Gateway](#) en la Guía para desarrolladores de API Gateway.

[APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (8), PCI DSS v4.0.1/10.4.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::ApiGatewayV2::Stage

Regla de AWS Config : [api-gwv2-access-logs-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las etapas de Amazon API Gateway V2 tienen configurado el registro de acceso. Este control falla si no se ha definido la configuración del registro de acceso.

Los registros de acceso a API Gateway proporcionan información detallada sobre quién ha obtenido acceso a la API y cómo la persona que llama ha obtenido acceso a la API. Estos registros son útiles para aplicaciones como las auditorías de seguridad y acceso y la investigación forense. Habilite estos registros de acceso para analizar los patrones de tráfico y solucionar problemas.

Para obtener más información sobre las prácticas recomendadas, consulte [Supervisión de REST APIs](#) en la Guía para desarrolladores de API Gateway.

Corrección

Para configurar el registro de acceso, consulte [Configurar el registro de CloudWatch API mediante la consola de API Gateway](#) en la Guía para desarrolladores de API Gateway.

Controles de Security Hub para AWS AppConfig

Estos controles de Security Hub evalúan el AWS AppConfig servicio y los recursos.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[AppConfig.1] AWS AppConfig las aplicaciones deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::AppConfig::Application

Regla de AWS Config: appconfig-application-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una AWS AppConfig aplicación tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si la aplicación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si la aplicación no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas, AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una AWS AppConfig aplicación, consulte [TagResource](#) en la Referencia de la API de AWS AppConfig .

[AppConfig.2] los perfiles de AWS AppConfig configuración deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::AppConfig::ConfigurationProfile`

Regla de AWS Config: `appconfig-configuration-profile-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un perfil de AWS AppConfig configuración tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el perfil de configuración no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el perfil de configuración no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un perfil de AWS AppConfig configuración, consulte [TagResource](#) en la Referencia de la API de AWS AppConfig .

[AppConfig.3] AWS AppConfig los entornos deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::AppConfig::Environment`

Regla de AWS Config : `appconfig-environment-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.		que cumplan con AWS los requisitos .	

Este control comprueba si un AWS AppConfig entorno tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el entorno no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el entorno no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas, AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un AWS AppConfig entorno, consulte [TagResource](#) en la Referencia de la API de AWS AppConfig .

[AppConfig.4] Las asociaciones AWS AppConfig de extensiones deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::AppConfig::ExtensionAssociation

Regla de AWS Config : appconfig-extension-association-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una asociación de AWS AppConfig extensiones tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si la asociación de extensiones no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y genera un error si la asociación de extensiones no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una asociación de AWS AppConfig extensiones, consulte [TagResource](#) en la Referencia de la API de AWS AppConfig .

Controles de Security Hub para Amazon AppFlow

Estos controles de Security Hub evalúan el AppFlow servicio y los recursos de Amazon.

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[AppFlow.1] AppFlow Los flujos de Amazon deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::AppFlow::Flow

Regla de AWS Config : appflow-flow-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un AppFlow flujo de Amazon tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el flujo no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el flujo no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para

obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un AppFlow flujo de Amazon, consulta [Crear flujos en Amazon AppFlow en](#) la Guía del AppFlow usuario de Amazon.

Controles de Security Hub para AWS App Runner

Estos AWS Security Hub controles evalúan el AWS App Runner servicio y los recursos. Es posible que los controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[AppRunner.1] Los servicios de App Runner deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::AppRunner::Service

Regla de AWS Config : [apprunner-service-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un AWS App Runner servicio tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el servicio App Runner no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y produce un error si el servicio de App Runner no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para obtener información sobre cómo añadir etiquetas a un AWS App Runner servicio, consulte [TagResource](#) en la Referencia de la API de AWS App Runner .

[AppRunner.2] Los conectores VPC de App Runner deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::AppRunner::VpcConnector

Regla de AWS Config : [apprunner-vpc-connector-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un conector de AWS App Runner VPC tiene etiquetas con las claves específicas definidas en el parámetro. `requiredKeyTags` El control falla si el conector de VPC no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro. `requiredKeyTags` Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el conector de VPC no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para obtener información sobre cómo añadir etiquetas a un conector de AWS App Runner VPC, consulte [TagResource](#) en la Referencia de la API de AWS App Runner .

Controles de Security Hub para AWS AppSync

Estos controles de Security Hub evalúan el AWS AppSync servicio y los recursos.

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[AppSync.1] Las cachés de las AWS AppSync API deben cifrarse en reposo

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::AppSync::GraphQLApi

Regla de AWS Config : [appsync-cache-ct-encryption-at-rest](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la caché de una AWS AppSync API está cifrada en reposo. El control falla si la caché de la API no está cifrada en reposo.

Los datos en reposo hacen referencia a los datos que se almacenan en un almacenamiento persistente y no volátil durante cualquier periodo de tiempo. El cifrado de datos en reposo permite proteger la confidencialidad de los datos, lo que reduce el riesgo de que un usuario no autorizado pueda acceder a ellos.

Corrección

No puedes cambiar la configuración de cifrado después de habilitar el almacenamiento en caché para tu AWS AppSync API. En su lugar, debe eliminar la caché y volver a crearla con el cifrado habilitado. Para obtener más información, consulte [Cifrado de caché](#), en la Guía para desarrolladores de AWS AppSync .

[AppSync.2] AWS AppSync debe tener habilitado el registro a nivel de campo

Requisitos relacionados: PCI DSS v4.0.1/10.4.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::AppSync::GraphQLApi

Regla de AWS Config : [appsync-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
fieldLoggingLevel	Nivel de registro del campo	Enum	ERROR, ALL, INFO, DEBUG	No default value

Este control comprueba si una AWS AppSync API tiene activado el registro a nivel de campo. Se produce un error en el control si el nivel de registro del solucionador de campos está establecido en Ninguno. A menos que se proporcionen valores personalizados de parámetros para indicar que se debe habilitar un tipo de registro específico, Security Hub genera un resultado válido si el nivel de registro del solucionador de campos es ERROR o ALL.

Puede utilizar el registro y las métricas para identificar, solucionar problemas y optimizar sus consultas de GraphQL. Activar el registro en AWS AppSync GraphQL te ayuda a obtener información detallada sobre las solicitudes y respuestas de la API, a identificar y responder a los problemas y a cumplir con los requisitos reglamentarios.

Corrección

Para activar el registro AWS AppSync, consulta [Instalación y configuración](#) en la Guía para AWS AppSync desarrolladores.

[AppSync.4] AWS AppSync APIs GraphQL debe estar etiquetado

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::AppSync::GraphQLApi

Regla de AWS Config : tagged-appsync-graphqlapi (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una API de AWS AppSync GraphQL tiene etiquetas con las claves específicas definidas en el parámetro. `requiredTagKeys` El control falla si la API de GraphQL no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la API de GraphQL no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws :`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una API de AWS AppSync GraphQL, consulta [TagResource](#) en la Referencia de la API de AWS AppSync .

[AppSync.5] AWS AppSync APIs GraphQL no debe autenticarse con claves de API

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, (7), NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6

Categoría: Proteger > Gestión del acceso seguro > Autenticación sin contraseña

Gravedad: alta

Tipo de recurso: AWS::AppSync::GraphQLApi

Regla de AWS Config : [appsync-authorization-check](#)

Tipo de horario: provocado por un cambio

Parámetros:

- AllowedAuthorizationTypes: AWS_LAMBDA, AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS (no personalizable)

Este control comprueba si la aplicación utiliza una clave de API para interactuar con una API de AWS AppSync GraphQL. El control falla si una API de AWS AppSync GraphQL se autentica con una clave de API.

Una clave de API es un valor codificado en tu aplicación que genera el AWS AppSync servicio al crear un punto final de GraphQL no autenticado. Si esta clave de API se ve comprometida, su punto

de conexión es vulnerable a un acceso no deseado. A menos que respalde una aplicación o un sitio web de acceso público, no recomendamos usar una clave de API para la autenticación.

Corrección

Para configurar una opción de autorización para tu API de AWS AppSync GraphQL, consulta [Autorización y autenticación](#) en la Guía para AWS AppSync desarrolladores.

[AppSync.6] Las cachés de las AWS AppSync API deben cifrarse en tránsito

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::AppSync::ApiCache

Regla de AWS Config : [appsync-cache-ct-encryption-in-transit](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la caché de una AWS AppSync API está cifrada en tránsito. El control falla si la caché de la API no está cifrada en tránsito.

Los datos en tránsito hacen referencia a los datos que se mueven de una ubicación a otra, por ejemplo, entre los nodos del clúster o entre el clúster y la aplicación. Los datos pueden moverse a través de Internet o dentro de una red privada. El cifrado de los datos en tránsito reduce el riesgo de que un usuario no autorizado pueda espiar el tráfico de la red.

Corrección

No puedes cambiar la configuración de cifrado después de habilitar el almacenamiento en caché para tu AWS AppSync API. En su lugar, debe eliminar la caché y volver a crearla con el cifrado habilitado. Para obtener más información, consulte [Cifrado de caché](#), en la Guía para desarrolladores de AWS AppSync .

Controles de Security Hub para Amazon Athena

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon Athena. Es posible que los controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Athena.1] Los grupos de trabajo de Athena deben estar cifrados en reposo

Important

Security Hub retiró este control en abril de 2024. Para obtener más información, consulte [Registro de cambios para los controles CSPM de Security Hub](#).

Categoría: Proteger - Protección de datos - Cifrado de datos en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Gravedad: media

Tipo de recurso: AWS::Athena::WorkGroup

Regla de AWS Config : [athena-workgroup-encrypted-at-rest](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de trabajo de Athena está cifrado en reposo. El control falla si un grupo de trabajo de Athena no está cifrado en reposo.

En Athena, puede crear grupos de trabajo para ejecutar consultas para equipos, aplicaciones o diferentes cargas de trabajo. Cada grupo de trabajo tiene una configuración que permite el cifrado de todas las consultas. Tiene la opción de utilizar el cifrado del lado del servidor con las claves administradas por Amazon Simple Storage Service (Amazon S3), el cifrado del lado del servidor con claves AWS Key Management Service (AWS KMS) o el cifrado del lado del cliente con claves de KMS administradas por el cliente. Los datos en reposo se refieren a cualquier dato que se almacene en un almacenamiento persistente y no volátil durante cualquier período de tiempo. El cifrado le ayuda a proteger la confidencialidad de dichos datos, reduciendo el riesgo de que un usuario no autorizado pueda acceder a ellos.

Corrección

Para habilitar el cifrado en reposo para los grupos de trabajo de Athena, consulte [Editar un grupo de trabajo](#) en la Guía del usuario de Amazon Athena. En la sección Configuración de los resultados de la consulta, seleccione Cifrar los resultados de la consulta.

[Athena.2] Los catálogos de datos de Athena deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Athena::DataCatalog

Regla de AWS Config : tagged-athena-datacatalog (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si el catálogo de datos de Amazon Athena tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el catálogo de datos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el catálogo de datos no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los

propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un catálogo de datos de Athena, consulte [Etiquetado de los recursos de Athena](#) en la Guía del usuario de Amazon Athena.

[Athena.3] Los grupos de trabajo de Athena deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Athena::WorkGroup

Regla de AWS Config : tagged-athena-workgroup (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si el grupo de trabajo de Amazon Athena tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el grupo de trabajo no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el grupo de trabajo no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre

ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un grupo de trabajo de Athena, consulte [Agregar y eliminar etiquetas en un grupo de trabajo individual](#) en la Guía del usuario de Amazon Athena.

[Athena.4] Los grupos de trabajo de Athena deben tener el registro habilitado

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::Athena::WorkGroup

Regla de AWS Config : [athena-workgroup-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de trabajo de Amazon Athena tiene activado el registro. El control falla si el grupo de trabajo no tiene habilitado el registro.

Los registros de auditoría rastrean y supervisan las actividades del sistema. Proporcionan un registro de los eventos que puede ayudarlo a detectar brechas de seguridad, investigar incidentes y cumplir con las normativas. Los registros de auditoría también mejoran la responsabilidad y la transparencia generales de su organización.

Corrección

Para obtener información sobre cómo habilitar el registro para un grupo de trabajo de Athena, consulte [Habilitar las métricas de CloudWatch consulta en Athena en la Guía del usuario](#) de Amazon Athena.

Controles de Security Hub para AWS Backup

Estos controles de Security Hub evalúan el AWS Backup servicio y los recursos.

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Backup.1] Los puntos AWS Backup de recuperación deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CP-9(8), NIST.800-53.r5 SI-12

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::Backup::RecoveryPoint

Regla de AWS Config : [backup-recovery-point-encrypted](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un punto AWS Backup de recuperación está cifrado en reposo. Se produce un error en el control si el punto de recuperación no está cifrado en reposo.

Un punto de AWS Backup recuperación hace referencia a una copia o instantánea específica de los datos que se crea como parte de un proceso de copia de seguridad. Representa un momento concreto en el que se hizo una copia de seguridad de los datos y sirve como punto de restauración en caso de que los datos originales se pierdan, se dañen o sean inaccesibles. El cifrado de los puntos de recuperación de la copia de seguridad agrega una capa adicional de protección contra el acceso no autorizado. El cifrado es la práctica recomendada para proteger la confidencialidad, la integridad y la seguridad de los datos de la copia de seguridad.

Corrección

Para cifrar un punto de AWS Backup recuperación, consulte [Cifrado de copias de seguridad AWS Backup en la Guía para AWS Backup](#) desarrolladores.

[Backup.2] Los puntos AWS Backup de recuperación deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Backup::RecoveryPoint

Regla de AWS Config: tagged-backup-recoverypoint (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un punto de AWS Backup recuperación tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el punto de recuperación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el punto de recuperación no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un punto de recuperación AWS Backup

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, seleccione Backup plans (Planes de copias de seguridad).
3. Seleccione un plan de copias de seguridad de la lista.
4. En la sección Etiquetas del plan de copias de seguridad, elija Administrar etiquetas.
5. Escriba la clave y el valor de para la etiqueta. Seleccione Agregar etiqueta nueva para agregar pares de clave-valor adicionales.
6. Cuando haya terminado de agregar etiquetas, elija Save (Guardar).

[Backup.3] las AWS Backup bóvedas deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Backup::BackupVault

Regla de AWS Config: tagged-backup-backupvault (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un AWS Backup depósito tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el punto de recuperación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el punto de recuperación no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre

ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un almacén AWS Backup

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Backup vaults (Almacenes de copia de seguridad).
3. Seleccione un almacén de copias de seguridad de la lista.
4. En la sección Etiquetas del almacén de copias de seguridad, elija Administrar etiquetas.
5. Escriba la clave y el valor de para la etiqueta. Seleccione Agregar etiqueta nueva para agregar pares de clave-valor adicionales.
6. Cuando haya terminado de agregar etiquetas, elija Save (Guardar).

[Backup.4] los planes de AWS Backup informes deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Backup::ReportPlan

Regla de AWS Config: tagged-backup-reportplan (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.		que cumplan con AWS los requisitos .	

Este control comprueba si un plan de AWS Backup informes tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el plan de informes no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el plan de informes no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws :`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un plan de informes AWS Backup

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Backup vaults (Almacenes de copia de seguridad).
3. Seleccione un almacén de copias de seguridad de la lista.
4. En la sección Etiquetas del almacén de copias de seguridad, elija Administrar etiquetas.
5. Elija Añadir nueva etiqueta. Escriba la clave y el valor de para la etiqueta. Repita la acción para pares de clave-valor adicionales.
6. Cuando haya terminado de agregar etiquetas, elija Save (Guardar).

[Backup.5] los planes de AWS Backup respaldo deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Backup::BackupPlan

Regla de AWS Config: tagged-backup-backupplan (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un plan AWS Backup de respaldo tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el plan de copias de seguridad no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el plan de copias de seguridad no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un plan de respaldo AWS Backup

1. Abra la AWS Backup consola en <https://console.aws.amazon.com/backup>.
2. En el panel de navegación, elija Backup vaults (Almacenes de copia de seguridad).
3. Seleccione un almacén de copias de seguridad de la lista.
4. En la sección Etiquetas del almacén de copias de seguridad, elija Administrar etiquetas.

5. Elija Añadir nueva etiqueta. Escriba la clave y el valor de para la etiqueta. Repita la acción para pares de clave-valor adicionales.
6. Cuando haya terminado de agregar etiquetas, elija Save (Guardar).

Controles de Security Hub para AWS Batch

Estos controles de Security Hub evalúan el AWS Batch servicio y los recursos. Es posible que los controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Batch.1] Las colas de trabajos por lotes deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Batch::JobQueue

Regla de AWS Config : [batch-job-queue-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una cola de AWS Batch trabajos tiene etiquetas con las claves específicas definidas en el parámetro. `requiredKeyTags` El control falla si la cola de trabajos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro. `requiredKeyTags` Si

`requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si la cola de trabajos no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas, AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una cola de trabajos de Batch, consulte [Etiquete sus recursos](#) en la Guía del AWS Batch usuario.

[Batch.2] Las políticas de programación de lotes deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Batch::SchedulingPolicy`

Regla de AWS Config : [batch-scheduling-policy-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una política de AWS Batch programación tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si la política de programación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si la política de programación no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una política de programación de Batch, consulte [Etiquete sus recursos](#) en la Guía del AWS Batch usuario.

[Batch.3] Los entornos de procesamiento por lotes deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Batch::ComputeEnvironment

Regla de AWS Config : [batch-compute-environment-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un entorno AWS Batch informático tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el entorno de cómputo no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el entorno de procesamiento no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas, AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un entorno de procesamiento por lotes, consulte [Etiquete sus recursos](#) en la Guía del AWS Batch usuario.

[Batch.4] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Batch::ComputeEnvironment

Regla de AWS Config : [batch-managed-compute-env-compute-resources-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Una lista de claves de etiquetas que no existen y que se deben asignar a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si la propiedad de los recursos informáticos de un entorno AWS Batch informático gestionado tiene las claves de etiqueta especificadas en el `requiredKeyTags` parámetro. El control produce un error si la propiedad de recursos de cálculo no tiene ninguna clave de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no especificas ningún valor para el `requiredKeyTags` parámetro, el control solo comprueba la existencia de una clave de etiqueta y produce un error si una propiedad de recursos de cálculo no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws:` prefijo. Este control no evalúa los entornos informáticos no gestionados ni los entornos gestionados que utilizan recursos. AWS Fargate

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarle a identificar, organizar, buscar y filtrar los recursos. También pueden ayudarte a realizar un seguimiento de las acciones y notificaciones de los propietarios de los recursos. También puedes usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para

obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas](#).

 Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están pensadas para usarse con datos privados o confidenciales.

Corrección

Para obtener información sobre cómo añadir etiquetas a los recursos informáticos en un entorno AWS Batch informático gestionado, [consulte Etiquetar los recursos](#) en la Guía del AWS Batch usuario.

Controles de Security Hub para AWS Certificate Manager

Estos AWS Security Hub controles evalúan el servicio y los recursos de AWS Certificate Manager (ACM). Es posible que los controles de no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[ACM.1] Los certificados importados y emitidos por ACM deben renovarse después de un período de tiempo específico

Requisitos relacionados: NIST.800-53.r5 SC-2 8 (3), NIST.800-53.r5 SC-7 (16), niST.800-171.r2 3.13.15, PCI DSS v4.0.1/4.2.1

Categoría: Protección > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::ACM::Certificate

Regla de AWS Config : [acm-certificate-expiration-check](#)

Tipo de programa: activado por cambios y periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
daysToExpiration	Número de días en los que se debe renovar el certificado de ACM	Entero	De 14 a 365	30

Este control comprueba si un certificado de AWS Certificate Manager (ACM) se renueva dentro del periodo especificado. Comprueba tanto los certificados importados como los certificados que proporciona ACM. Se produce un error en el control si el certificado no se renueva en el periodo especificado. A menos que se proporcione un valor personalizado de parámetro para el periodo de renovación, Security Hub utiliza un valor predeterminado de 30 días.

ACM puede renovar automáticamente los certificados que utilizan la validación de DNS. En el caso de los certificados que utilizan la validación por correo electrónico, debe responder a un correo electrónico de validación de dominio. ACM no renueva automáticamente los certificados que se importan. Debe renovar los certificados importados manualmente.

Corrección

ACM proporciona renovación administrada para sus certificados SSL/TLS emitidos por Amazon. Esto significa que ACM renueva sus certificados de forma automática (si utiliza la validación por DNS) o le envía avisos por correo electrónico cuando se acerque la fecha de vencimiento. Estos servicios se prestan tanto para certificados de ACM públicos como privados.

Para dominios validados por correo electrónico

Cuando un certificado expira 45 días, ACM envía al propietario del dominio un correo electrónico para cada nombre de dominio. Para validar los dominios y completar la renovación, debe responder a las notificaciones por correo electrónico.

Para obtener más información, consulte [Renovación de dominios validados por correo electrónico](#) en la Guía del usuario de AWS Certificate Manager .

Para dominios validados por DNS

ACM renueva automáticamente los certificados que utilizan la validación de DNS. 60 días antes del vencimiento, ACM verifica que el certificado se pueda renovar.

Si no puede validar un nombre de dominio, ACM envía una notificación indicando que es necesaria la validación manual. Envía estas notificaciones 45 días, 30 días, 7 días y 1 día antes de la fecha de vencimiento.

Para obtener más información, consulte [Renovación de dominios validados por DNS](#) en la AWS Certificate Manager Guía del usuario de .

[ACM.2] Los certificados RSA administrados por ACM deben utilizar una longitud de clave de al menos 2048 bits

Requisitos relacionados: PCI DSS v4.0.1/4.2.1

Categoría: Identificar > Inventario > Servicios de inventario

Gravedad: alta

Tipo de recurso: AWS::ACM::Certificate

Regla de AWS Config : [acm-certificate-rsa-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los certificados RSA administrados por AWS Certificate Manager utilizan una longitud de clave de al menos 2048 bits. El control falla si la longitud de la clave es inferior a 2048 bits.

La fuerza del cifrado se correlaciona directamente con el tamaño de la clave. Recomendamos una longitud de clave de al menos 2048 bits para sus AWS recursos de, ya que la potencia de cálculo se abarata y los servidores se vuelven más avanzados.

Corrección

La longitud mínima de clave para los certificados RSA emitidos por ACM ya es de 2048 bits. Para obtener instrucciones sobre cómo emitir nuevos certificados RSA con ACM, consulte [Emisión y administración de certificados](#) en la Guía del usuario de AWS Certificate Manager .

Si bien ACM le permite importar certificados con longitudes de clave más cortas, debe utilizar claves de al menos 2048 bits para pasar este control. No se puede cambiar la longitud de la clave después de importar un certificado. En su lugar, debe eliminar los certificados con una longitud de clave inferior a 2048 bits. Para obtener más información sobre la importación de certificados en ACM, consulte [Prerrequisitos para importar certificados](#) en la Guía del usuario de AWS Certificate Manager.

[ACM.3] Los certificados ACM deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::ACM::Certificate

Regla de AWS Config : tagged-acm-certificate (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un certificado de AWS Certificate Manager (ACM) tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el certificado no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el certificado no está etiquetado con

ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un certificado ACM, consulte [Etiquetado de AWS Certificate Manager certificados](#) en la Guía del usuario.AWS Certificate Manager

Controles de Security Hub para AWS CloudFormation

Estos controles de Security Hub evalúan el AWS CloudFormation servicio y los recursos.

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[CloudFormation.1] las CloudFormation pilas deben integrarse con el Simple Notification Service (SNS)

Important

Security Hub retiró este control en abril de 2024. Para obtener más información, consulte [Registro de cambios para los controles CSPM de Security Hub](#).

Requisitos relacionados: NIST.800-53.r5 SI-4(12), NIST.800-53.r5 SI-4(5)

Categoría: Detectar > Servicios de detección > Supervisión de aplicaciones

Gravedad: baja

Tipo de recurso: AWS::CloudFormation::Stack

Regla de AWS Config : [cloudformation-stack-notification-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una notificación de Amazon Simple Notification Service está integrada con una pila de AWS CloudFormation . Se produce un error en el control de una CloudFormation pila si no hay ninguna notificación de SNS asociada a ella.

La configuración de una notificación de SNS con su CloudFormation pila ayuda a notificar inmediatamente a las partes interesadas cualquier evento o cambio que se produzca en la pila.

Corrección

Para integrar una CloudFormation pila y un tema de SNS, consulte [Actualización de pilas directamente](#) en la Guía del AWS CloudFormation usuario.

[CloudFormation.2] las CloudFormation pilas deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::CloudFormation::Stack`

Regla de AWS Config : `tagged-cloudformation-stack` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una AWS CloudFormation pila tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la pila no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la pila no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una CloudFormation pila, consulta la referencia [CreateStack](#) de la AWS CloudFormation API.

Controles les les les les les les les les les les les les les les les les CloudFront

Estos AWS Security Hub controles de evalúan el CloudFront servicio y los recursos de Amazon. Es posible que los controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[CloudFront.1] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado

Requisitos relacionados: NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), PCI DSS v4.0.1/2.2.6

Categoría: Proteger > Gestión del acceso seguro > Recursos que no son de acceso público

Gravedad: alta

Tipo de recurso: AWS::CloudFront::Distribution

Regla de AWS Config : [cloudfront-default-root-object-configured](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una CloudFront distribución de Amazon está configurada para devolver un objeto específico que es el objeto raíz predeterminado. El control falla si la CloudFront distribución no tiene configurado un objeto raíz predeterminado.

A veces, un usuario puede solicitar la URL raíz de la distribución en lugar de un objeto de la distribución. Cuando esto ocurre, especificar un objeto raíz predeterminado puede ayudarle a evitar la exposición del contenido de su distribución web.

Corrección

Para configurar un objeto raíz predeterminado para una CloudFront distribución, consulte [Cómo especificar un objeto raíz predeterminado](#) en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.3] CloudFront las distribuciones deben requerir el cifrado en tránsito

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3 (3), (NIST.800-53.r5 SC-13), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), PCI DSS v4.0.1/4.2.1

Categoría: Protección > Protección > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::CloudFront::Distribution

Regla de AWS Config : [cloudfront-viewer-policy-https](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una CloudFront distribución de Amazon requiere que los espectadores utilicen HTTPS directamente o si utiliza la redirección. El control falla si ViewerProtocolPolicy está configurado como allow-all para defaultCacheBehavior o para cacheBehaviors.

HTTPS (TLS) puede utilizarse para ayudar a evitar posibles ataques person-in-the-middle o similares para espiar o manipular el tráfico de red. Solo se deben permitir las conexiones cifradas a través de HTTPS (TLS). El cifrado de los datos en tránsito puede afectar al rendimiento. Debe probar su aplicación con esta característica para comprender el perfil de rendimiento y el impacto del TLS.

Corrección

Para cifrar una CloudFront distribución en tránsito, consulte [Exigir HTTPS para la comunicación entre espectadores y CloudFront](#) en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.4] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: baja

Tipo de recurso: AWS::CloudFront::Distribution

Regla de AWS Config : [cloudfront-origin-failover-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una CloudFront distribución de Amazon está configurada con un grupo de origen que tiene dos o más orígenes.

CloudFront La conmutación por error de origen puede aumentar la disponibilidad. La conmutación por error de Origin redirige automáticamente el tráfico a un origen secundario si el origen principal no está disponible o si devuelve códigos de estado de respuesta HTTP específicos.

Corrección

Para configurar la conmutación por error de origen para una CloudFront distribución, consulta [Cómo crear un grupo de origen](#) en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront5] CloudFront las distribuciones deben tener el registro habilitado

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), (9), NIST.800-53.r5 AC-4 NIST.800-53.r5 SI-3 NIST.800-53.r5 AC-6 (8), NIST.800-53.r5 NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7 SI-7 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-7 (8), NIST.800-53.r5 SI-7 (8), NIST.800-53.r5 SI-7 (8), NIST.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::CloudFront::Distribution

Regla de AWS Config : [cloudfront-accesslogs-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el registro de acceso al servidor está habilitado en CloudFront las distribuciones. El control falla si el registro de acceso no está habilitado para una distribución. Este control solo evalúa si el registro estándar (heredado) está habilitado para una distribución.

CloudFront Los registros de acceso proporcionan información detallada sobre cada solicitud de usuario que CloudFront recibe. Cada registro contiene información como la fecha y la hora en que se recibió la solicitud, la dirección IP del espectador que realizó la solicitud, el origen de la solicitud y el número de puerto de la solicitud del espectador. Estos registros son útiles para aplicaciones como auditorías de seguridad y acceso y para investigaciones forenses. Para obtener más información sobre el análisis de los registros de acceso, consulte [Consulta CloudFront los registros de Amazon](#) en la Guía del usuario de Amazon Athena.

Corrección

Para configurar el registro estándar (heredado) para una CloudFront distribución, consulte [Configurar el registro estándar \(heredado\)](#) en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.6] CloudFront Las distribuciones deben tener WAF habilitado

Requisitos relacionados: NIST.800-53.r5 AC-4 (21), PCI DSS v4.0.1/6.4.2

Categoría: Proteger > Servicios de protección

Gravedad: media

Tipo de recurso: AWS::CloudFront::Distribution

Regla de AWS Config : [cloudfront-associated-with-waf](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si CloudFront las distribuciones están asociadas a la AWS WAF versión clásica o AWS WAF web ACLs. El control falla si la distribución no está asociada a una ACL web.

AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones web y APIs los ataques. Le permite configurar un conjunto de reglas denominadas lista de control de acceso web

(Web ACL) que permiten, bloquean o cuentan solicitudes web en función de las reglas y condiciones de seguridad web personalizables que defina. Asegúrese de que su CloudFront distribución esté asociada a una ACL AWS WAF web de para protegerla de ataques maliciosos.

Corrección

Para asociar una ACL AWS WAF web a una CloudFront distribución, consulte [Uso AWS WAF para controlar el acceso a su contenido](#) en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.7] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, 2 NIST.800-53.r5 IA-5 (3), 3, 3 (3), (3), NIST.800-53.r5 SC-1 (4), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-2 (NIST.800-53.r5 SC-12), NIST.800-53.r5 SC-7 Nist.800-53.r5 NIST.800-53.r5 SC-8 SI-7 NIST.800-53.r5 SC-8 (6), NIST.800-53.r5 SC-8 Nist.800-171.r2 3.13.15

Categoría: Protección > Protección > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::CloudFront::Distribution

Regla de AWS Config : [cloudfront-custom-ssl-certificate](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si CloudFront las distribuciones utilizan el SSL/TLS certificate CloudFront provides. This control passes if the CloudFront distribution uses a custom SSL/TLS certificate. This control fails if the CloudFront distribution uses the default SSL/TLS certificado predeterminado.

Los SSL/TLS personalizados permiten a los usuarios acceder al contenido mediante nombres de dominio alternativos. Puede almacenar los certificados personalizados en AWS Certificate Manager (recomendado) o en IAM.

Corrección

Para añadir un nombre de dominio alternativo a una CloudFront distribución mediante un certificado SSL/TLS personalizado, consulte [Añadir un nombre de dominio alternativo en](#) la Guía para desarrolladores de Amazon. CloudFront

[CloudFront.8] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Proteger - Configuración de red segura

Gravedad: baja

Tipo de recurso: AWS::CloudFront::Distribution

Regla de AWS Config : [cloudfront-sni-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si CloudFront las distribuciones de Amazon utilizan un método de SSL/TLS certificate and are configured to use SNI to serve HTTPS requests. This control fails if a custom SSL/TLS certificate is associated but the SSL/TLS soporte personalizado es una dirección IP dedicada.

Server Name Indication (SNI) (Indicación de nombre de servidor [SNI]) es una extensión del protocolo TLS que admiten los navegadores y clientes disponibles desde 2010. Si configura CloudFront para atender solicitudes HTTPS mediante SNI, CloudFront asocia el nombre de dominio alternativo a una dirección IP para cada ubicación de borde. Cuando un espectador envía una solicitud HTTPS de contenido, el servicio DNS dirige la solicitud a la dirección IP de la ubicación de borde correcta. La dirección IP de su nombre de dominio se determina durante la negociación del protocolo SSL/TLS; la dirección IP no es exclusiva de su distribución.

Corrección

Para configurar una CloudFront distribución para usar SNI para atender solicitudes HTTPS, consulte [Uso de SNI para atender solicitudes HTTPS \(funciona para la mayoría de los clientes\)](#) en la Guía para CloudFront desarrolladores. Para obtener información sobre certificados SSL personalizados, consulte [Requisitos para el uso de certificados SSL/TLS](#) con. CloudFront

[CloudFront.9] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3 (3), (NIST.800-53.r5 SC-13), NIST.800-53.r5 SC-2 (4),

NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8
NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), PCI DSS v4.0.1/4.2.1

Categoría: Protección > Protección > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::CloudFront::Distribution

Regla de AWS Config : [cloudfront-traffic-to-origin-encrypted](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si CloudFront las distribuciones de Amazon cifran el tráfico hacia orígenes personalizados. Este control falla en una CloudFront distribución cuya política de protocolo de origen permite «solo http». Este control también falla si la política de protocolo de origen de la distribución es “match-viewer”, mientras que la política de protocolo de visor es “permisible para todos”.

El protocolo HTTPS (TLS) se puede utilizar para evitar el espionaje o la manipulación del tráfico de la red. Solo se deben permitir las conexiones cifradas a través de HTTPS (TLS).

Corrección

Para actualizar la política de protocolo de origen para exigir el cifrado de una CloudFront conexión, consulte [Exigir HTTPS para la comunicación entre CloudFront y su origen personalizado](#) en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.10] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), (2) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (2), (NIST.800-53.r5 SC-12), (2), NIST.800-53.r5 SC-1 (2), NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (4), NIST.800-171.r2 3.13.15, PCI DSS v4.0.1/4.2.1

Categoría: Protección > Protección > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::CloudFront::Distribution

Regla de AWS Config : [cloudfront-no-deprecated-ssl-protocols](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si CloudFront las distribuciones de Amazon utilizan protocolos SSL obsoletos para la comunicación HTTPS entre las ubicaciones CloudFront periféricas y sus orígenes personalizados. Este control falla si una CloudFront distribución tiene un «CustomOriginConfig where OriginSslProtocols includes». SSLv3

En 2015, el Internet Engineering Task Force (IETF) anunció oficialmente que el SSL 3.0 debería quedar obsoleto debido a que el protocolo no era lo suficientemente seguro. Se recomienda utilizar TLSv1.2 o una versión posterior para la comunicación HTTPS con sus orígenes personalizados.

Corrección

Para actualizar los protocolos SSL de origen para una CloudFront distribución, consulte [Exigir HTTPS para la comunicación entre CloudFront y su origen personalizado](#) en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.12] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), PCI DSS v4.0.1/2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.2.6

Categoría: Identificar > Configuración de recursos

Gravedad: alta

Tipo de recurso: AWS::CloudFront::Distribution

Regla de AWS Config : [cloudfront-s3-origin-non-existent-bucket](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si CloudFront las distribuciones de Amazon apuntan a orígenes de Amazon S3 inexistentes. El control falla en una CloudFront distribución si el origen está configurado para apuntar a un bucket inexistente. Este control solo se aplica a CloudFront las distribuciones en las que el origen de S3 es un bucket de S3 sin alojamiento de sitios web estáticos.

Cuando una CloudFront distribución de su cuenta está configurada para apuntar a un bucket que no existe, un tercero malintencionado puede crear el bucket al que se hace referencia y publicar su propio contenido a través de su distribución. Recomendamos comprobar todos los orígenes, independientemente del comportamiento de enrutamiento, para asegurarse de que sus distribuciones apuntan a los orígenes adecuados.

Corrección

Para modificar una CloudFront distribución para que apunte a un nuevo origen, consulta [Actualización de una distribución](#) en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.13] CloudFront Las distribuciones deben usar el control de acceso de origen

Categoría: Proteger > Gestión del acceso seguro > Recurso no accesible públicamente

Gravedad: media

Tipo de recurso: AWS::CloudFront::Distribution

Regla de AWS Config : [cloudfront-s3-origin-access-control-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una CloudFront distribución de Amazon con origen en Amazon S3 tiene configurado el Control de acceso de origen (OAC). El control falla si el OAC no está configurado para la CloudFront distribución.

Si utiliza un bucket de S3 como origen para la CloudFront distribución, puede habilitar OAC. Esto permite el acceso al contenido del bucket únicamente a través de la CloudFront distribución especificada y prohíbe el acceso directo desde el bucket u otra distribución. Si bien CloudFront admite identidad de acceso de origen (OAI), OAC ofrece funciones adicionales y las distribuciones que utilizan OAI pueden migrar a OAC. Si bien la OAI proporciona una forma segura de acceder a los orígenes de S3, presenta limitaciones, como la falta de compatibilidad con configuraciones de políticas pormenorizadas y con solicitudes HTTP/HTTPS que utilizan el método POST en y Regiones de AWS que requieren AWS Signature Version 4 (Signature Version 4). La OAI tampoco admite el cifrado con AWS Key Management Service. La OAC se basa en la práctica de AWS recomendada de utilizar las entidades principales del servicio de IAM para autenticarse con orígenes S3.

Corrección

Para configurar OAC para una CloudFront distribución con orígenes S3, consulte [Restricción del acceso a un origen de Amazon S3](#) en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.14] CloudFront Las distribuciones deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::CloudFront::Distribution

AWS Config Regla: tagged-cloudfront-distribution (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una CloudFront distribución de Amazon tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la distribución no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la distribución no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una CloudFront distribución, consulta Cómo [etiquetar CloudFront distribuciones de Amazon](#) en la Guía para CloudFront desarrolladores de Amazon.

Controles de Security Hub para AWS CloudTrail

Estos AWS Security Hub controles evalúan el AWS CloudTrail servicio y los recursos. Es posible que los controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[CloudTrail.1] CloudTrail debe habilitarse y configurarse con al menos un registro de seguimiento para varias regiones que incluya eventos de administración de lectura y escritura

Requisitos relacionados: Indicador de referencia AWS de de CIS v1.2.0/2.1, Indicador de referencia de de CIS AWS v1.4.0/3.1, Indicador de referencia de de CIS AWS v3.0.0/3.1, NIST.800-53.r5 AC-2 (4), (26), (9),, NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (22) NIST.800-53.r5 AU-10,

NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-14(1), NIST.800-53.r5 CA-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8), NIST.800-53.r5 SA-8

Categoría: Identificar - Registro

Gravedad: alta

Tipo de recurso: AWS : : : Account

Regla de AWS Config : [multi-region-cloudtrail-enabled](#)

Tipo de programa: Periódico

Parámetros:

- `readWriteType`: ALL (no personalizable)
- `includeManagementEvents`: true (no personalizable)

Este control comprueba si existe al menos un registro de seguimiento de varias regiones AWS CloudTrail que capture eventos de administración de lectura y escritura. El control lanza error si CloudTrail está deshabilitado o si no hay al menos un CloudTrail registro de seguimiento que capture eventos de administración de lectura y escritura.

AWS CloudTrail registra las llamadas a la AWS API de de para su cuenta y proporciona archivos de registro. La información registrada incluye lo siguiente:

- Identidad del intermediario de la API
- Hora de la llamada a la API
- Dirección IP de origen de la persona que llama a la API
- Parámetros de solicitud
- Elementos de respuesta devueltos por Servicio de AWS

CloudTrail proporciona un historial de llamadas a la AWS API de para una cuenta, incluidas las llamadas a la API realizadas desde las herramientas de línea de comandos de AWS Management Console AWS SDKs,. El historial también incluye llamadas de la API desde de nivel superior Servicios de AWS como AWS CloudFormation.

El historial de llamadas a la AWS API producido por CloudTrail permite realizar análisis de seguridad, seguimientos de cambios en los recursos y auditorías de conformidad. Los registros de seguimiento de varias regiones también ofrecen los siguientes beneficios.

- Un registro de seguimiento de varias regiones ayuda a detectar la actividad inesperada que ocurre en regiones que no se utilizan.
- Un registro de seguimiento de eventos de varias regiones garantiza que el registro de servicios globales esté habilitado para un registro de seguimiento de forma predeterminada. El registro de eventos de servicios globales registra los eventos generados por los servicios AWS globales.
- Para un registro de seguimiento de varias regiones, los eventos de administración para todas las operaciones de lectura y escritura garantizan que las operaciones de administración de CloudTrail registren en todos los recursos de una Cuenta de AWS cuenta de.

De forma predeterminada, las CloudTrail rutas que se crean usando AWS Management Console son rutas de varias regiones.

Corrección

Para crear un nuevo sendero multirregional CloudTrail, consulte [Creación de un sendero](#) en la Guía del AWS CloudTrail usuario. Use los siguientes valores:

Campo	Valor
Configuración adicional: validación de archivos de registro	Habilitado
Elija los eventos de registro, los eventos de administración y la actividad de la API	Leer y Escribir. Desactive las casillas de verificación de las exclusiones.

Para actualizar una ruta existente, consulte [Actualización de una ruta](#) en la Guía del usuario de AWS CloudTrail . En Eventos de administración, para la actividad de la API, seleccione Leer y Escribir.

[CloudTrail.2] CloudTrail debe tener habilitado el cifrado en reposo

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/2.7, CIS AWS Foundations Benchmark v1.4.0/3.7, CIS Foundations Benchmark v3.0.0/3.5, NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8 NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), (10),

NIS.800-53.r5 SI-7 (6), NIST.800-53.r5 SC-2 NIS.800-171.r2 3.3.8, NIST.800-53.r5 SC-7 PCI AWS DSS v3.2.1/3.4, PCI DSS v4.0.1/3.2

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::CloudTrail::Trail

Regla de AWS Config : [cloud-trail-encryption-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si CloudTrail se ha configurado para utilizar el cifrado del servidor (SSE). AWS KMS key El control falla si no se ha definido KmsKeyId.

Para obtener una capa adicional de seguridad para los archivos de CloudTrail registro confidenciales, debe utilizar el [cifrado del servidor con AWS KMS keys \(SSE-KMS\)](#) para los archivos de CloudTrail registro para el cifrado en reposo. Tenga en cuenta que los archivos de registro que envían CloudTrail a sus buckets se cifran mediante el sistema de [Amazon de cifrado del servidor con claves de cifrado administradas mediante Amazon S3 \(SSE-S3\)](#).

Corrección

Para habilitar el cifrado SSE-KMS para los archivos de registro, consulte [Actualizar un CloudTrail registro para usar una clave KMS en la Guía del usuario](#).AWS CloudTrail

[CloudTrail.3] Al menos un CloudTrail registro de seguimiento debe habilitarse

Requisitos relacionados: NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.14.6, PCI DSS v3.2.1/10.1, PCI DSS v3.2.1/10.1, PCI DSS v3.2.1/10.2.1, PCI DSS v3.2.1/10.2.2, PCI DSS v3.2.1/10.2.3, PCI DSS v3.2.1/10.2.4, PCI DSS v3.2.1/10.2.4, PCI DSS v3.2.1/10.2.4, PCI DSS v3.2.1/10.2.4, PCI DSS v3.2.1/10.2.4, PCI DSS v3.2.1/10.2.4, PCI DSS v3.2.1/10.2.4, PCI DSS v3.2.1/10.2.4 2.1/10.2.5, PCI DSS v3.2.1/10.2.6, PCI DSS v3.2.1/10.2.7, PCI DSS v3.2.1/10.3.1, PCI DSS v3.2.1/10.3.3, PCI DSS v3.2.1/10.3.3, PCI DSS v3.2.1/10.3.5, PCI DSS v3.2.1/10.3.5, PCI DSS v3.2.1/10.3.6, PCI DSS v4.0.1/10.2.1

Categoría: Identificar - Registro

Gravedad: alta

Tipo de recurso: AWS:::Account

Regla de AWS Config : [cloudtrail-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un AWS CloudTrail registro de seguimiento de está habilitado en su cuenta de Cuenta de AWS. El control lanza error si su cuenta no tiene al menos un CloudTrail registro de seguimiento habilitado.

Sin embargo, algunos AWS servicios no permiten el registro de todos APIs los eventos. Debe implementar cualquier registro de auditoría adicional que no sea CloudTrail y revisar la documentación de cada servicio en [Servicios e integraciones CloudTrail compatibles](#).

Corrección

Para empezar CloudTrail a crear un registro, consulte el [AWS CloudTrail tutorial Cómo empezar a usarlo](#) en la Guía del AWS CloudTrail usuario.

[CloudTrail.4] La validación de archivo de CloudTrail registro debe estar habilitada

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/2.2, CIS Foundations Benchmark v1.4.0/3.2, CIS AWS Foundations Benchmark v3.0.0/3.2, NIS.800-53.r5, NIS.800-53.r5 SI-4, NIS.800-53.r5 SI-7 (1), NIS.800-53.r5 SI-7 (3), NIS.800-53.r5 SI-7 (3), NIS.800-53.r5 ST.800-171.r2 3.3.8, PCI AWS DSS v3.2.1/10.5.2, PCI DSS v3.2.1/10.5.5, PCI DSS v4.0.1/10.3.2

Categoría: Protección de datos > Integridad de los datos

Gravedad: baja

Tipo de recurso: AWS::CloudTrail::Trail

Regla de AWS Config : [cloud-trail-log-file-validation-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la validación de la integridad del archivo de registro está habilitada en un registro CloudTrail de seguimiento.

CloudTrail La validación de archivos de registro crea un archivo de resumen firmado digitalmente que contiene un hash de cada registro que CloudTrail escribe en Amazon S3. Puede utilizar estos

archivos de resumen para determinar si un archivo de registro se ha modificado, eliminado o sigue igual después de CloudTrail entregar el registro.

Recomendamos que Hub recomienda que habilite la validación de archivos en todos los registros de seguimiento. La validación de archivos de registro proporciona una comprobación de integridad adicional de CloudTrail los registros.

Corrección

Para habilitar CloudTrail la validación de la integridad de los archivos de [registro, consulte Habilitar la validación de la integridad de los archivos](#) de registro CloudTrail en la Guía del AWS CloudTrail usuario de.

[CloudTrail.5] CloudTrail Los senderos deben estar integrados con Amazon Logs CloudWatch

Requisitos relacionados: PCI DSS v3.2.1/10.5.3, CIS AWS Foundations Benchmark v1.2.0/2.4, CIS Foundations Benchmark v1.4.0/3.4, NIST.800-53.r5 AC-2 (4), (9), (9), NIS.800-53.r5 SI-20, NIS.800-53.r5 SI-3 (8), NIST.800-53.r5 AC-4 NIS.800-53.r5 SI-4 NIST.800-53.r5 AC-6 (20), NIS.800-53.r5 SI-4 NIST.800-53.r5 SC-7 (20), NIS.800-53.r5 5 SI-4 (5), NIST.800-53.r5 SI-7 (8) AWS NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 AU-7(1), NIST.800-53.r5 CA-7

Categoría: Identificar - Registro

Gravedad: baja

Tipo de recurso: AWS::CloudTrail::Trail

Regla de AWS Config : [cloud-trail-cloud-watch-logs-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si los registros CloudTrail de seguimiento de están configurados para enviar CloudWatch registros a. El control falla si la propiedad CloudWatchLogsLogGroupArn de la ruta está vacía.

CloudTrail registra las llamadas a la AWS API de que se realizan en una cuenta determinada. La información registrada incluye lo siguiente:

- Identidad de la persona que llama a la API
- Hora de la llamada a la API
- Dirección IP de origen de la persona que llama a la API
- Parámetros de solicitudes
- Elementos de respuesta devueltos por Servicio de AWS

CloudTrail utiliza Amazon S3 para el almacenamiento y la entrega de archivos de registro. Puede capturar CloudTrail registros en un bucket de S3 específico para analizarlos a largo plazo. Para realizar análisis en tiempo real, puede CloudTrail configurar el envío de CloudWatch registros a.

Para un registro de seguimiento que está habilitado en todas las regiones de una cuenta, CloudTrail envía archivos de registro de todas esas regiones a un grupo de CloudWatch registros.

Security Hub recomienda enviar CloudTrail CloudWatch registros a. Tenga en cuenta que esta recomendación tiene por objeto garantizar que la actividad de la cuenta se capture, supervise y se genere la alarma adecuada. Puede utilizar CloudWatch los registros para configurar esto con su Servicios de AWS. Esta recomendación no impide el uso de una solución diferente.

Enviar CloudTrail CloudWatch registros a Logs facilita el registro de actividad histórico y en tiempo real en función del usuario, la API, el recurso y la dirección IP. Puede utilizar este abordaje para establecer alarmas y notificaciones en caso de que se produzcan actividades de la cuenta anómalas o delicadas.

Corrección

Para integrarlo CloudTrail con CloudWatch los registros, consulte [Enviar eventos a CloudWatch los registros](#) en la Guía del AWS CloudTrail usuario.

[CloudTrail.6] Asegurar que los CloudTrail registros del bucket de S3 no son de acceso público

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/2.3, CIS Foundations Benchmark v1.4.0/3.3, PCI AWS DSS v4.0.1/1.4.4

Categoría: Identificar - Registro

Gravedad: crítica

Tipo de recurso: AWS::S3::Bucket

AWS Config Regla de: Ninguna (regla personalizada de Security Hub)

Tipo de programa: periódico y activado por cambios

Parámetros: ninguno

CloudTrail lleva un registro de cada llamada a la API en su cuenta. Los archivos de registro se almacenan en un bucket de S3. CIS recomienda que la política de bucket o la lista de control de acceso (ACL) que se aplica al bucket de S3 que CloudTrail registra para impedir el acceso público a los CloudTrail registros. Permitir el acceso público al contenido de los CloudTrail registros podría ayudar a un adversario a identificar los puntos débiles del uso o de la configuración de la cuenta afectada.

Para ejecutar esta comprobación, Security Hub utiliza primero la lógica personalizada para buscar el bucket de S3 en el que se almacenan CloudTrail los registros. A continuación, utiliza las reglas AWS Config administradas para comprobar que el depósito es de acceso público.

Si agrega sus registros en un único bucket de S3 centralizado, Security Hub solo realizará la comprobación de la cuenta y la región en las que se encuentra el bucket de S3 centralizado. En el caso de otras cuentas y regiones, el estado de control es Sin datos.

Si el bucket está accesible públicamente, la comprobación genera un resultado de error.

Corrección

Para bloquear el acceso público a su bucket de CloudTrail S3, consulte [Configuración de los ajustes de bloqueo de acceso público para sus buckets de S3](#) en la Guía del usuario de Amazon Simple Storage Service. Seleccione las cuatro configuraciones de Bloqueo de acceso público de Amazon S3.

[CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el bucket de CloudTrail S3

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/2.6, CIS Foundations Benchmark v1.4.0/3.6, CIS AWS Foundations Benchmark v3.0.0/3.4, PCI DSS v4.0.1/10.2.1 AWS

Categoría: Identificar - Registro

Gravedad: baja

Tipo de recurso: AWS::S3::Bucket

AWS Config Regla de: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

El registro de acceso al bucket S3 genera un registro que contiene registros de acceso para cada solicitud realizada a su bucket S3. Un registro de acceso contiene detalles sobre la solicitud, como el tipo de solicitud, los recursos especificados en la solicitud con los que se ha trabajado y la fecha y hora en que se procesó la solicitud.

CIS recomienda que habilite el registro de acceso al bucket en el bucket de CloudTrail S3.

Al habilitar el registro del bucket de S3 en los buckets de S3 de destino, puede capturar todos los eventos que podrían afectar a los objetos en el bucket de destino. Configurar los registros para que se coloquen en un bucket independiente permite el acceso a la información de registro, lo que puede resultar útil en flujos de trabajo de respuesta a incidentes y seguridad.

Para ejecutar esta comprobación, Security Hub utiliza primero la lógica personalizada para buscar el bucket en el que se almacenan CloudTrail los registros y, a continuación, utiliza la regla AWS Config administrada para comprobar si el registro está habilitado.

Si CloudTrail entrega archivos de registro de varias Cuentas de AWS a un único bucket de Amazon S3, Security Hub evalúa este control únicamente en comparación con el bucket de destino de la región en la que se encuentra. Esto optimiza sus resultados. Sin embargo, debe habilitarse CloudTrail en todas las cuentas que entreguen registros al bucket de destino. Para todas las cuentas, excepto la que contiene el bucket de destino, el estado de control es Sin datos.

Corrección

Para habilitar el registro de acceso al servidor para su bucket de CloudTrail S3, consulte [Habilitar el registro de acceso al servidor Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.

[CloudTrail.9] los registros de CloudTrail seguimiento deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::CloudTrail::Trail

Regla de AWS Config : tagged-cloudtrail-trail (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un AWS CloudTrail registro de seguimiento de tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el registro de seguimiento no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el registro de seguimiento no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una CloudTrail ruta, consulta la referencia [AddTags](#) de la AWS CloudTrail API.

[CloudTrail.10] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el cliente AWS KMS keys

Requisitos relacionados: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-1 2 (2), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-2 8 (1), Nist.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::CloudTrail::EventDataStore

Regla de AWS Config : [event-data-store-cmk-encryption-enabled](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
kmsKeyArns	Una lista de los nombres de recursos de	StringList (máximo de 3 elementos)	De 1 a 3 ARNs de las claves KMS existente	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	Amazon (ARNs) AWS KMS keys para incluirlos en la evaluación. El control genera un FAILED resultado si el almacén de datos de un evento no está cifrado con una clave KMS de la lista.		s. Por ejemplo: arn:aws:kms:us-west-2:11112223333:key/1234abcd-12ab-34cd-56ef-1234567890ab .	

Este control comprueba si un almacén de datos de eventos de AWS CloudTrail Lake está cifrado en reposo con un sistema administrado por el cliente AWS KMS key. El control falla si el almacén de datos del evento no está cifrado con una clave KMS administrada por el cliente. Si lo desea, puede especificar una lista de claves de KMS para que el control las incluya en la evaluación.

De forma predeterminada, AWS CloudTrail Lake cifra los registros de datos de eventos con claves administradas de Amazon S3 (SSE-S3) mediante un algoritmo AES-256. Para tener un control adicional, puede configurar CloudTrail Lake para que cifre un almacén de datos de eventos mediante un sistema gestionado por el cliente (SSE-KMS). AWS KMS key Una clave de KMS administrada por el cliente es una clave AWS KMS key que usted ha creado, posee y administra en su Cuenta de AWS. Usted tiene el control total sobre este tipo de clave de KMS. Esto incluye definir y mantener la política de claves, administrar las concesiones, rotar el material criptográfico, asignar etiquetas, crear alias y habilitar y deshabilitar la clave. Puede utilizar una clave KMS gestionada por el cliente en las operaciones criptográficas para sus CloudTrail datos y auditar el uso de los registros. CloudTrail

Corrección

Para obtener información sobre cómo cifrar un banco de datos de eventos de AWS CloudTrail Lake con una AWS KMS key que usted especifique, consulte [Actualizar un banco de datos de eventos](#)

[en la](#) Guía del AWS CloudTrail usuario. Después de asociar un almacén de datos de eventos a una clave de KMS, esta no se podrá eliminar ni cambiar.

Controles de Security Hub CloudWatch

Estos AWS Security Hub controles de evalúan el CloudWatch servicio y los recursos de Amazon. Es posible que los controles de no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[CloudWatch.1] Debe existir un filtro de métricas de registro y una alarma para el uso del usuario «raíz»

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/1.1, CIS Foundations Benchmark v1.2.0/3.3, CIS AWS Foundations Benchmark v1.4.0/1.7, CIS Foundations Benchmark v1.4.0/4.3, AWS NIST.800-171.R2 3.14.6, NIST.800-171.r2 3.14.7, PCI DSS AWS v3.2.1/7.2.1

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::Logs::MetricFilter, AWS::CloudWatch::Alarm, AWS::CloudTrail::Trail, AWS::SNS::Topic

AWS Config Regla de: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Este usuario raíz tiene acceso a todos los recursos y los servicios no restringidos de Cuenta de AWS. Le recomendamos encarecidamente que evite utilizar el usuario raíz para las tareas diarias. Cuanto menos se use el usuario raíz y cuanto más se adopte el principio de otorgar privilegios mínimos para la administración del acceso, más se reduce el riesgo de que se produzcan cambios accidentales y la divulgación no deseada de credenciales con muchos privilegios.

Como práctica recomendada, utilice sus credenciales de usuario raíz solo cuando sea necesario para [realizar tareas de administración de cuentas y servicios](#). Aplique políticas de AWS Identity and Access Management (IAM) directamente a los grupos y roles, pero no a los usuarios. Para ver un tutorial sobre cómo configurar un administrador para el uso diario, consulte [Creación del primer grupo y usuario administrador de IAM](#) en la Guía de usuario de IAM.

Para ejecutar esta comprobación, Security Hub utiliza la lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 1.7 en [CIS AWS Foundations Benchmark v1.4.0](#). Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

 Note

Cuando Security Hub comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organización que pertenezcan a otra cuenta. Las rutas multirregionales también pueden estar basadas en una Región diferente. La comprobación arroja resultados de FAILED en los siguientes casos:

- No hay ningún rastro configurado.
- Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.

La comprobación da como resultado un estado de control de NO_DATA en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub solo puede generar resultados en la Región en la que se encuentra el rastro.
- Una ruta multirregional pertenece a una cuenta diferente. Security Hub solo puede generar resultados para la cuenta propietaria de la ruta.

Recomendamos los registros de la organización para registrar los eventos de muchas cuentas de una organización. Las rutas de organización son rutas multirregionales de forma predeterminada y solo las puede gestionar la cuenta AWS Organizations de administración de o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de NO_DATA de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub solo genera resultados para los recursos propiedad de los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a

`ListSubscriptionsByTopic`. De lo contrario, Security Hub generará resultados de WARNING para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte [Crear un registro de seguimiento](#) en la Guía del usuario de AWS CloudTrail .

Anote el nombre del grupo de CloudWatch registros de registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulta Cómo [crear un filtro de métricas para un grupo de registros](#) en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{\$.userIdentity.type="Root" && \$.userIdentity.invokedBy NOT EXISTS && \$.eventType != "AwsServiceEvent"}</code>
Espacio de nombres de métrica	LogMetrics
Valor de la métrica	1
Valor predeterminado	0

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulta Cómo [crear una CloudWatch alarma basada en un filtro métrico de grupo de registros](#) en la Guía CloudWatch del usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... <i>your-metric-name</i>	Mayor/Igual
que...	1

[CloudWatch.2] Asegurar que haya un filtro de métricas de registro y alarma para las llamadas a la API no autorizadas

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.1, NIST.800-171.r2 3.13.1, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::Logs::MetricFilter, AWS::CloudWatch::Alarm, AWS::CloudTrail::Trail, AWS::SNS::Topic

AWS Config Regla de: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo CloudTrail los registros a CloudWatch los registros y estableciendo los filtros de métricas y alarmas correspondientes.

CIS recomienda que cree un filtro de métricas y alarma para las llamadas a la API no autorizadas. La monitorización de las llamadas no autorizadas a la API ayuda a revelar errores de la aplicación y puede reducir el tiempo que se tarda en detectar actividades malintencionadas.

Para ejecutar esta comprobación, Security Hub utiliza la lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 3.1 en [CIS AWS Foundations Benchmark v1.2](#). Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

 Note

Cuando Security Hub comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organización que pertenezcan a otra cuenta. Las rutas multirregionales también pueden estar basadas en una Región diferente. La comprobación arroja resultados de FAILED en los siguientes casos:

- No hay ningún rastro configurado.
- Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.

La comprobación da como resultado un estado de control de NO_DATA en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub solo puede generar resultados en la Región en la que se encuentra el rastro.
- Una ruta multirregional pertenece a una cuenta diferente. Security Hub solo puede generar resultados para la cuenta propietaria de la ruta.

Recomendamos los registros de la organización para registrar los eventos de muchas cuentas de una organización. Las rutas de organización son rutas multirregionales de forma predeterminada y solo las puede gestionar la cuenta AWS Organizations de administración de o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de NO_DATA de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub solo genera resultados para los recursos propiedad de los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub generará resultados de WARNING para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte [Crear un registro de seguimiento](#) en la Guía del usuario de AWS CloudTrail .

Anote el nombre del grupo de CloudWatch registros de registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulta Cómo [crear un filtro de métricas para un grupo de registros](#) en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{{\$.errorCode="*UnauthorizedOperation" (\$.errorCode="AccessDenied*")}}</code>
Espacio de nombres de métrica	LogMetrics
Valor de la métrica	1
Valor predeterminado	0

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulta Cómo [crear una CloudWatch alarma basada en un filtro métrico de grupo de registros](#) en la Guía CloudWatch del usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... <i>your-metric-name</i>	Mayor/Igual

Campo	Valor
que...	1

[CloudWatch.3] Asegurar que haya un filtro de métricas de registro y alarma de registro para el inicio de sesión en la Consola de administración sin MFA

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::Logs::MetricFilter, AWS::CloudWatch::Alarm, AWS::CloudTrail::Trail, AWS::SNS::Topic

AWS Config Regla de: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo CloudTrail los registros a CloudWatch los registros y estableciendo los filtros de métricas y alarmas correspondientes.

CIS recomienda que cree un filtro de métricas y alarma para los inicios de sesión en la consola que no estén protegidos por MFA. La monitorización de los inicios de sesión de la consola con un solo factor aumenta la visibilidad de las cuentas que no están protegidas por MFA.

Para ejecutar esta comprobación, Security Hub utiliza la lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 3.2 en [CIS AWS Foundations Benchmark v1.2](#). Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

Note

Cuando Security Hub comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organización que pertenezcan a otra cuenta. Las rutas multirregionales también pueden estar basadas en una Región diferente.

La comprobación arroja resultados de FAILED en los siguientes casos:

- No hay ningún rastro configurado.
- Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.

La comprobación da como resultado un estado de control de NO_DATA en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub solo puede generar resultados en la Región en la que se encuentra el rastro.
- Una ruta multirregional pertenece a una cuenta diferente. Security Hub solo puede generar resultados para la cuenta propietaria de la ruta.

Recomendamos los registros de la organización para registrar los eventos de muchas cuentas de una organización. Las rutas de organización son rutas multirregionales de forma predeterminada y solo las puede gestionar la cuenta AWS Organizations de administración de o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de NO_DATA de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub solo genera resultados para los recursos propiedad de los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub generará resultados de WARNING para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte [Crear un registro de seguimiento](#) en la Guía del usuario de AWS CloudTrail .

Anote el nombre del grupo de CloudWatch registros de registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulta Cómo [crear un filtro de métricas para un grupo de registros](#) en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<pre>{ (\$.eventName = "ConsoleLogin") && (\$.additionalEventData.MFAUsed != "Yes") && (\$.userIdentity.type = "IAMUser") && (\$.responseElements.ConsoleLogin = "Success") }</pre>
Espacio de nombres de métrica	LogMetrics
Valor de la métrica	1
Valor predeterminado	0

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulta Cómo [crear una CloudWatch alarma basada en un filtro métrico de grupo de registros](#) en la Guía CloudWatch del usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... <i>your-metric-name</i>	Mayor/Igual

Campo	Valor
que...	1

[CloudWatch.4] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de IAM

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.4, CIS Foundations Benchmark v1.4.0/4.4, NIST.800-171.r2 AWS 3.14.6, 800-171.r2 3.14.7

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regla de: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si monitorizas las llamadas a la API en tiempo real. Para ello, dirige CloudTrail los registros a CloudWatch los registros y establece los filtros de métricas y las alarmas correspondientes.

CIS recomienda que cree un filtro de métricas y alarma para los cambios realizados a las políticas de IAM. La monitorización de estos cambios ayuda a garantizar que los controles de autenticación y autorización permanezcan intactos.

Note

Cuando Security Hub comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organización que pertenezcan a otra cuenta. Las rutas multirregionales también pueden estar basadas en una Región diferente. La comprobación arroja resultados de FAILED en los siguientes casos:

- No hay ningún rastro configurado.

- Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.

La comprobación da como resultado un estado de control de NO_DATA en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub solo puede generar resultados en la Región en la que se encuentra el rastro.
- Una ruta multirregional pertenece a una cuenta diferente. Security Hub solo puede generar resultados para la cuenta propietaria de la ruta.

Recomendamos los registros de la organización para registrar los eventos de muchas cuentas de una organización. Las rutas de organización son rutas multirregionales de forma predeterminada y solo las puede gestionar la cuenta AWS Organizations de administración de o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de NO_DATA de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub solo genera resultados para los recursos propiedad de los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub generará resultados de WARNING para el control.

Corrección

Note

El patrón de filtro que recomendamos en estos pasos de corrección difiere del patrón de filtro de la guía del CIS. Nuestros filtros recomendados se dirigen únicamente a los eventos que provienen de las llamadas a la API de IAM.

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte [Crear un registro de seguimiento](#) en la Guía del usuario de AWS CloudTrail .

Anote el nombre del grupo de CloudWatch registros de registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulta Cómo [crear un filtro de métricas para un grupo de registros](#) en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<pre>{ (\$.eventSource=iam.amazonaws.com) && ((\$.eventName=DeleteGroupPolicy) (\$.eventName=DeleteRolePolicy) (\$.eventName=DeleteUserPolicy) (\$.eventName=PutGroupPolicy) (\$.eventName=PutRolePolicy) (\$.eventName=PutUserPolicy) (\$.eventName=CreatePolicy) (\$.eventName=DeletePolicy) (\$.eventName=CreatePolicyVersion) (\$.eventName=DeletePolicyVersion) (\$.eventName=AttachRolePolicy) (\$.eventName=DetachRolePolicy) (\$.eventName=AttachUserPolicy) (\$.eventName=DetachUserPolicy) (\$.eventName=AttachGroupPol</pre>

Campo	Valor
	icy) (\$.eventName=DetachGroupPolicy))}
Espacio de nombres de métrica	LogMetrics
Valor de la métrica	1
Valor predeterminado	0

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulta Cómo [crear una CloudWatch alarma basada en un filtro métrico de grupo de registros](#) en la Guía CloudWatch del usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... <i>your-metric-name</i>	Mayor/Igual
que...	1

[CloudWatch.5] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de CloudTrail configuración de

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.5, CIS Foundations Benchmark v1.4.0/4.5, NIST.800-171.r2 3.3.8, AWS NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::Logs::MetricFilter, AWS::CloudWatch::Alarm, AWS::CloudTrail::Trail, AWS::SNS::Topic

AWS Config Regla de: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo CloudTrail los registros a CloudWatch los registros y estableciendo los filtros de métricas y alarmas correspondientes.

CIS recomienda que cree un filtro de métricas y alarma para los cambios a los ajustes de la configuración de CloudTrail. La monitorización de estos cambios ayuda a garantizar la visibilidad continua de las actividades de la cuenta.

Para ejecutar esta comprobación, Security Hub utiliza la lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.5 en [CIS AWS Foundations Benchmark v1.4.0](#). Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

 Note

Cuando Security Hub comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organización que pertenezcan a otra cuenta. Las rutas multirregionales también pueden estar basadas en una Región diferente. La comprobación arroja resultados de FAILED en los siguientes casos:

- No hay ningún rastro configurado.
- Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.

La comprobación da como resultado un estado de control de NO_DATA en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub solo puede generar resultados en la Región en la que se encuentra el rastro.
- Una ruta multirregional pertenece a una cuenta diferente. Security Hub solo puede generar resultados para la cuenta propietaria de la ruta.

Recomendamos los registros de la organización para registrar los eventos de muchas cuentas de una organización. Las rutas de organización son rutas multirregionales de forma predeterminada y solo las puede gestionar la cuenta AWS Organizations de administración de o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de NO_DATA de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub solo genera resultados para los recursos propiedad de los

miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub generará resultados de WARNING para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte [Crear un registro de seguimiento](#) en la Guía del usuario de AWS CloudTrail .

Anote el nombre del grupo de CloudWatch registros de registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulta Cómo [crear un filtro de métricas para un grupo de registros](#) en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<pre>{(\$.eventName=CreateTrail) (\$.eventName=UpdateTrail) (\$.eventName>DeleteTrail) (\$.eventName=StartLogging) (\$.eventName=StopLogging)}</pre>
Espacio de nombres de métrica	LogMetrics

Campo	Valor
Valor de la métrica	1
Valor predeterminado	0

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulta Cómo [crear una CloudWatch alarma basada en un filtro métrico de grupo de registros](#) en la Guía CloudWatch del usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... <i>your-metric-name</i>	Mayor/Igual
que...	1

[CloudWatch.6] Asegurar que haya un filtro de métricas de registro y alarma de registro para los errores de AWS Management Console autenticación

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.6, CIS Foundations Benchmark v1.4.0/4.6, NIST.800-171.r2 AWS 3.14.6, 800-171.r2 3.14.7

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::Logs::MetricFilter, AWS::CloudWatch::Alarm, AWS::CloudTrail::Trail, AWS::SNS::Topic

AWS Config Regla de: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo CloudTrail los registros a CloudWatch los registros y estableciendo los filtros de métricas y alarmas correspondientes.

CIS recomienda que cree un filtro de métrica y alarma para los intentos de autenticación de la consola que producen un error. La monitorización de los inicios de sesión con error en la consola podría disminuir el tiempo que se tarda en detectar un intento introducir credenciales por fuerza bruta, lo que podría proporcionar un indicador, como el IP de origen, que se puede utilizar en otras correlaciones de eventos.

Para ejecutar esta comprobación, Security Hub utiliza la lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.6 en [CIS AWS Foundations Benchmark v1.4.0](#). Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

Note

Cuando Security Hub comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organización que pertenezcan a otra cuenta. Las rutas multirregionales también pueden estar basadas en una Región diferente. La comprobación arroja resultados de FAILED en los siguientes casos:

- No hay ningún rastro configurado.
- Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.

La comprobación da como resultado un estado de control de NO_DATA en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub solo puede generar resultados en la Región en la que se encuentra el rastro.
- Una ruta multirregional pertenece a una cuenta diferente. Security Hub solo puede generar resultados para la cuenta propietaria de la ruta.

Recomendamos los registros de la organización para registrar los eventos de muchas cuentas de una organización. Las rutas de organización son rutas multirregionales de forma predeterminada y solo las puede gestionar la cuenta AWS Organizations de administración de o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de NO_DATA de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub solo genera resultados para los recursos propiedad de los miembros. Los resultados relacionados con los registros de la organización se generan

en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub generará resultados de WARNING para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte [Crear un registro de seguimiento](#) en la Guía del usuario de AWS CloudTrail .

Anote el nombre del grupo de CloudWatch registros de registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulta Cómo [crear un filtro de métricas para un grupo de registros](#) en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{{\$.eventName=ConsoleLogin)&& (\$.errorMessage="Failed authentication")}}</code>
Espacio de nombres de métrica	LogMetrics
Valor de la métrica	1
Valor predeterminado	0

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulta [Cómo crear una CloudWatch alarma basada en un filtro métrico de grupo de registros](#) en la Guía CloudWatch del usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... <i>your-metric-name</i>	Mayor/Igual
que...	1

[CloudWatch.7] Asegurar que haya un filtro de métricas de registro y alarma de registro para la deshabilitación o eliminación programada de claves administradas por el cliente

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.7, CIS Foundations Benchmark v1.4.0/4.7, NIST.800-171.r2 3.13.10 AWS, NIST.800-171.r2 3.13.16, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::Logs::MetricFilter, AWS::CloudWatch::Alarm, AWS::CloudTrail::Trail, AWS::SNS::Topic

AWS Config Regla de: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo CloudTrail los registros a CloudWatch los registros y estableciendo los filtros de métricas y alarmas correspondientes.

CIS recomienda que cree un filtro de métricas y alarma para claves administradas por el cliente que hayan cambiado de estado a deshabilitada o eliminación programada. Los datos cifrados con claves deshabilitadas o eliminadas ya no son accesibles.

Para ejecutar esta comprobación, Security Hub utiliza la lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.7 en [CIS AWS Foundations Benchmark v1.4.0](#). Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas. El control también falla si `ExcludeManagementEventSources` contiene `kms.amazonaws.com`.

Note

Cuando Security Hub comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organización que pertenezcan a otra cuenta. Las rutas multirregionales también pueden estar basadas en una Región diferente. La comprobación arroja resultados de FAILED en los siguientes casos:

- No hay ningún rastro configurado.
- Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.

La comprobación da como resultado un estado de control de NO_DATA en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub solo puede generar resultados en la Región en la que se encuentra el rastro.
- Una ruta multirregional pertenece a una cuenta diferente. Security Hub solo puede generar resultados para la cuenta propietaria de la ruta.

Recomendamos los registros de la organización para registrar los eventos de muchas cuentas de una organización. Las rutas de organización son rutas multirregionales de forma predeterminada y solo las puede gestionar la cuenta AWS Organizations de administración de o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de NO_DATA de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub solo genera resultados para los recursos propiedad de los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub generará resultados de WARNING para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail, un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte [Crear un registro de seguimiento](#) en la Guía del usuario de AWS CloudTrail.

Anote el nombre del grupo de CloudWatch registros de registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulta Cómo [crear un filtro de métricas para un grupo de registros](#) en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{{\$.eventSource=kms.amazonaws.com) && (\$.eventName=DisableKey) (\$.eventName=ScheduleKeyDeletion)}}</code>
Espacio de nombres de métrica	LogMetrics
Valor de la métrica	1
Valor predeterminado	0

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulta [Cómo crear una CloudWatch alarma basada en un filtro métrico de grupo de registros](#) en la Guía CloudWatch del usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... <i>your-metric-name</i>	Mayor/Igual
que...	1

[CloudWatch.8] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de bucket de S3

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.8, CIS Foundations Benchmark v1.4.0/4.8, NIST.800-171.r2 AWS 3.14.6, 800-171.r2 3.14.7

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::Logs::MetricFilter, AWS::CloudWatch::Alarm, AWS::CloudTrail::Trail, AWS::SNS::Topic

AWS Config Regla de: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo CloudTrail los registros a CloudWatch los registros y estableciendo los filtros de métricas y alarmas correspondientes.

CIS recomienda que cree un filtro de métricas y alarma para los cambios realizados a las políticas de bucket S3. La monitorización de estos cambios puede reducir el tiempo que se tarda en detectar y corregir políticas permisivas sobre buckets de S3 confidenciales.

Para ejecutar esta comprobación, Security Hub utiliza la lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.8 en [CIS AWS Foundations Benchmark v1.4.0](#). Este

control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

 Note

Cuando Security Hub comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organización que pertenezcan a otra cuenta. Las rutas multirregionales también pueden estar basadas en una Región diferente. La comprobación arroja resultados de FAILED en los siguientes casos:

- No hay ningún rastro configurado.
- Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.

La comprobación da como resultado un estado de control de NO_DATA en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub solo puede generar resultados en la Región en la que se encuentra el rastro.
- Una ruta multirregional pertenece a una cuenta diferente. Security Hub solo puede generar resultados para la cuenta propietaria de la ruta.

Recomendamos los registros de la organización para registrar los eventos de muchas cuentas de una organización. Las rutas de organización son rutas multirregionales de forma predeterminada y solo las puede gestionar la cuenta AWS Organizations de administración de o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de NO_DATA de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub solo genera resultados para los recursos propiedad de los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a

`ListSubscriptionsByTopic`. De lo contrario, Security Hub generará resultados de WARNING para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte [Crear un registro de seguimiento](#) en la Guía del usuario de AWS CloudTrail .

Anote el nombre del grupo de CloudWatch registros de registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulta Cómo [crear un filtro de métricas para un grupo de registros](#) en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<pre>{(\$.eventSource=s3.amazonaws.com) && ((\$.eventName=PutBucketAcl) (\$.eventName=PutBucketPolicy) (\$.eventName=PutBucketCors) (\$.eventName=PutBucketLifecycle) (\$.eventName=PutBucketReplication) (\$.eventName=DeleteBucketPolicy) (\$.eventName=DeleteBucketCors) (\$.eventName=DeleteBucketLifecycle) (\$.eventName=DeleteBucketReplication))}</pre>

Campo	Valor
Espacio de nombres de métrica	LogMetrics
Valor de la métrica	1
Valor predeterminado	0

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulta Cómo [crear una CloudWatch alarma basada en un filtro métrico de grupo de registros](#) en la Guía CloudWatch del usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... <i>your-metric-name</i>	Mayor/Igual
que...	1

[CloudWatch.9] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de AWS Config configuración de

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.9, CIS Foundations Benchmark v1.4.0/4.9, NIST.800-171.r2 3.3.8, AWS NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::Logs::MetricFilter, AWS::CloudWatch::Alarm, AWS::CloudTrail::Trail, AWS::SNS::Topic

AWS Config Regla de: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo CloudTrail los registros a CloudWatch los registros y estableciendo los filtros de métricas y alarmas correspondientes.

CIS recomienda que cree un filtro de métricas y alarma para los cambios a los ajustes de la configuración de AWS Config . La monitorización de estos cambios ayuda a garantizar la visibilidad continua de los elementos de configuración de la cuenta.

Para ejecutar esta comprobación, Security Hub utiliza la lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.9 en [CIS AWS Foundations Benchmark v1.4.0](#). Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

Note

Cuando Security Hub comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organización que pertenezcan a otra cuenta. Las rutas multirregionales también pueden estar basadas en una Región diferente. La comprobación arroja resultados de FAILED en los siguientes casos:

- No hay ningún rastro configurado.
- Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.

La comprobación da como resultado un estado de control de NO_DATA en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub solo puede generar resultados en la Región en la que se encuentra el rastro.
- Una ruta multirregional pertenece a una cuenta diferente. Security Hub solo puede generar resultados para la cuenta propietaria de la ruta.

Recomendamos los registros de la organización para registrar los eventos de muchas cuentas de una organización. Las rutas de organización son rutas multirregionales de forma predeterminada y solo las puede gestionar la cuenta AWS Organizations de administración de o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de NO_DATA de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub solo genera resultados para los recursos propiedad de los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub generará resultados de WARNING para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail, un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte [Crear un registro de seguimiento](#) en la Guía del usuario de AWS CloudTrail.

Anote el nombre del grupo de CloudWatch registros de registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulta Cómo [crear un filtro de métricas para un grupo de registros](#) en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{{\$.eventSource=config.amazonaws.com) && (\$.eventName=StopConfigurationRecorder) (\$.eventName=DeleteDeliveryChannel) (\$.eventName=PutDeliveryChannel) (\$.eventName=PutConfigurationRecorder)}}</code>
Espacio de nombres de métrica	LogMetrics

Campo	Valor
Valor de la métrica	1
Valor predeterminado	0

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulta Cómo [crear una CloudWatch alarma basada en un filtro métrico de grupo de registros](#) en la Guía CloudWatch del usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... <i>your-metric-name</i>	Mayor/Igual
que...	1

[CloudWatch.10] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de grupos de seguridad

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.10, CIS Foundations Benchmark v1.4.10, NIST.800-171.r2 3.14.6, AWS NIST.800-171.r2 3.14.7

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::Logs::MetricFilter, AWS::CloudWatch::Alarm, AWS::CloudTrail::Trail, AWS::SNS::Topic

AWS Config Regla de: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo CloudTrail los registros a CloudWatch los registros y estableciendo los filtros de métricas y alarmas correspondientes. Los

grupos de seguridad son un filtro de paquetes con estado que controlan el tráfico de entrada y salida en una VPC.

CIS recomienda que cree un filtro de métricas y alarma para los cambios realizados a los grupos de seguridad. La monitorización de estos cambios ayuda a garantizar que los recursos y servicios no se expongan de forma involuntaria.

Para ejecutar esta comprobación, Security Hub utiliza la lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.10 en [CIS AWS Foundations Benchmark v1.4.0](#). Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

Note

Cuando Security Hub comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organización que pertenezcan a otra cuenta. Las rutas multirregionales también pueden estar basadas en una Región diferente. La comprobación arroja resultados de FAILED en los siguientes casos:

- No hay ningún rastro configurado.
- Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.

La comprobación da como resultado un estado de control de NO_DATA en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub solo puede generar resultados en la Región en la que se encuentra el rastro.
- Una ruta multirregional pertenece a una cuenta diferente. Security Hub solo puede generar resultados para la cuenta propietaria de la ruta.

Recomendamos los registros de la organización para registrar los eventos de muchas cuentas de una organización. Las rutas de organización son rutas multirregionales de forma predeterminada y solo las puede gestionar la cuenta AWS Organizations de administración de o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de NO_DATA de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub solo genera resultados para los recursos propiedad de los

miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub generará resultados de WARNING para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte [Crear un registro de seguimiento](#) en la Guía del usuario de AWS CloudTrail .

Anote el nombre del grupo de CloudWatch registros de registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulta Cómo [crear un filtro de métricas para un grupo de registros](#) en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{(\$.eventName=AuthorizeSecurityGroupIngress) (\$.eventName=AuthorizeSecurityGroupEgress) (\$.eventName=RevokeSecurityGroupIngress) (\$.eventName=RevokeSecurityGroupEgress) (\$.eventName>CreateSecurityGroup) </code>

Campo	Valor
	<code>(\$.eventName>DeleteSecurityGroup)}</code>
Espacio de nombres de métrica	LogMetrics
Valor de la métrica	1
Valor predeterminado	0

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulta Cómo [crear una CloudWatch alarma basada en un filtro métrico de grupo de registros](#) en la Guía CloudWatch del usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... <i>your-metric-name</i>	Mayor/Igual
que...	1

[CloudWatch.11] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios en las listas de control de acceso a la red (NACL)

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.11, CIS Foundations Benchmark v1.4.4.11, NIST.800-171.r2 3.14.6, AWS NIST.800-171.r2 3.14.7

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regla de: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo CloudTrail los registros a CloudWatch los registros y estableciendo los filtros de métricas y alarmas correspondientes. NACLs se utilizan como un filtro de paquetes sin estado para controlar el tráfico de entrada y salida de las subredes de una VPC.

CIS recomienda que cree un filtro de métricas y alarma para los cambios realizados a NACLs. La supervisión de estos cambios ayuda a garantizar que AWS los recursos y servicios no queden expuestos involuntariamente.

Para ejecutar esta comprobación, Security Hub utiliza la lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.11 en [CIS AWS Foundations Benchmark v1.4.0](#). Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

Note

Cuando Security Hub comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organización que pertenezcan a otra cuenta. Las rutas multirregionales también pueden estar basadas en una Región diferente. La comprobación arroja resultados de FAILED en los siguientes casos:

- No hay ningún rastro configurado.
- Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.

La comprobación da como resultado un estado de control de NO_DATA en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub solo puede generar resultados en la Región en la que se encuentra el rastro.
- Una ruta multirregional pertenece a una cuenta diferente. Security Hub solo puede generar resultados para la cuenta propietaria de la ruta.

Recomendamos los registros de la organización para registrar los eventos de muchas cuentas de una organización. Las rutas de organización son rutas multirregionales de forma predeterminada y solo las puede gestionar la cuenta AWS Organizations de administración de o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de NO_DATA de los controles

evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub solo genera resultados para los recursos propiedad de los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub generará resultados de WARNING para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail, un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte [Crear un registro de seguimiento](#) en la Guía del usuario de AWS CloudTrail.

Anote el nombre del grupo de CloudWatch registros de registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulta Cómo [crear un filtro de métricas para un grupo de registros](#) en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{ (\$.eventName=CreateNetworkAcl) (\$.eventName=CreateNetworkAclEntry) (\$.eventName>DeleteNetworkAcl) (\$.eventName>DeleteNetworkAclEntry) (\$.eventName=Repla</code>

Campo	Valor
	<code>ceNetworkAclEntry) (\$.eventName=ReplaceNetworkAclAssociation)}</code>
Espacio de nombres de métrica	LogMetrics
Valor de la métrica	1
Valor predeterminado	0

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulta Cómo [crear una CloudWatch alarma basada en un filtro métrico de grupo de registros](#) en la Guía CloudWatch del usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... <i>your-metric-name</i>	Mayor/Igual
que...	1

[CloudWatch.12] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a las puertas de enlace de la red

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.12, CIS Foundations Benchmark v1.4.4.12, NIST.800-171.r2 3.3.1, AWS NIST.800-171.r2 3.13.1

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regla de: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo CloudTrail los registros a CloudWatch los registros y estableciendo los filtros de métricas y alarmas correspondientes. Las gateways de red son necesarias para enviar y recibir tráfico a un destino fuera de una VPC.

CIS recomienda que cree un filtro de métricas y alarma para los cambios realizados a las puertas de enlace de red. La monitorización de estos cambios ayuda a garantizar que todo el tráfico de entrada y salida atraviesa la frontera de la VPC a través de una ruta controlada.

Para ejecutar esta comprobación, Security Hub utiliza la lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.12 en [CIS AWS Foundations Benchmark v1.2](#). Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

Note

Cuando Security Hub comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organización que pertenezcan a otra cuenta. Las rutas multirregionales también pueden estar basadas en una Región diferente. La comprobación arroja resultados de FAILED en los siguientes casos:

- No hay ningún rastro configurado.
- Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.

La comprobación da como resultado un estado de control de NO_DATA en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub solo puede generar resultados en la Región en la que se encuentra el rastro.
- Una ruta multirregional pertenece a una cuenta diferente. Security Hub solo puede generar resultados para la cuenta propietaria de la ruta.

Recomendamos los registros de la organización para registrar los eventos de muchas cuentas de una organización. Las rutas de organización son rutas multirregionales de forma predeterminada y solo las puede gestionar la cuenta AWS Organizations de administración de o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de NO_DATA de los controles

evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub solo genera resultados para los recursos propiedad de los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub generará resultados de **WARNING** para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail, un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte [Crear un registro de seguimiento](#) en la Guía del usuario de AWS CloudTrail.

Anote el nombre del grupo de CloudWatch registros de registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulta Cómo [crear un filtro de métricas para un grupo de registros](#) en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{ (\$.eventName=CreateCustomerGateway) (\$.eventName>DeleteCustomerGateway) (\$.eventName=AttachInternetGateway) (\$.eventName>CreateInternetGateway) (\$.eventName>Delete</code>

Campo	Valor
	<code>eInternetGateway) (\$.eventName=DetachInternetGateway)}</code>
Espacio de nombres de métrica	LogMetrics
Valor de la métrica	1
Valor predeterminado	0

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulta Cómo [crear una CloudWatch alarma basada en un filtro métrico de grupo de registros](#) en la Guía CloudWatch del usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... <i>your-metric-name</i>	Mayor/Igual
que...	1

[CloudWatch.13] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios ala tabla de enrutamiento

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.13, CIS Foundations Benchmark v1.4.4.13, NIST.800-171.r2 3.3.1, AWS NIST.800-171.r2 3.13.1, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regla de: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si monitorizas las llamadas a la API en tiempo real. Para ello, dirige CloudTrail los registros a CloudWatch los registros y establece los filtros de métricas y las alarmas correspondientes. Las tablas de enrutamiento dirigen el tráfico de red entre subredes y a gateways de red.

CIS recomienda que cree un filtro de métricas y alarma para los cambios realizados a las tablas de enrutamiento. La monitorización de estos cambios ayuda a garantizar que todo el tráfico de la VPC vaya a través de una ruta esperada.

Note

Cuando Security Hub comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organización que pertenezcan a otra cuenta. Las rutas multirregionales también pueden estar basadas en una Región diferente. La comprobación arroja resultados de FAILED en los siguientes casos:

- No hay ningún rastro configurado.
- Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.

La comprobación da como resultado un estado de control de NO_DATA en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub solo puede generar resultados en la Región en la que se encuentra el rastro.
- Una ruta multirregional pertenece a una cuenta diferente. Security Hub solo puede generar resultados para la cuenta propietaria de la ruta.

Recomendamos los registros de la organización para registrar los eventos de muchas cuentas de una organización. Las rutas de organización son rutas multirregionales de forma predeterminada y solo las puede gestionar la cuenta AWS Organizations de administración de o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de NO_DATA de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub solo genera resultados para los recursos propiedad de los miembros. Los resultados relacionados con los registros de la organización se generan

en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub generará resultados de WARNING para el control.

Corrección

Note

El patrón de filtro que recomendamos en estos pasos de corrección difiere del patrón de filtro de la guía del CIS. Nuestros filtros recomendados se centran únicamente en eventos procedentes de llamadas a la API Amazon Elastic Compute Cloud (EC2).

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree un CloudTrail registro que se aplique a todas Regiones de AWS. Para obtener instrucciones, consulte [Crear un registro de seguimiento](#) en la Guía del usuario de AWS CloudTrail .

Anote el nombre del grupo de CloudWatch registros de registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulta Cómo [crear un filtro de métricas para un grupo de registros](#) en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{{\$.eventSource=ec2.amazonaws.com) && ((\$.eventName=CreateRoute) (\$.eventName=CreateRouteTable) (\$.eventName=ReplaceRoute) (\$.eventName=ReplaceRouteTableAssociation) (\$.eventName>DeleteRouteTable) (\$.eventName>DeleteRoute) (\$.eventName=DisassociateRouteTable))}}</code>
Espacio de nombres de métrica	LogMetrics
Valor de la métrica	1
Valor predeterminado	0

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulta Cómo [crear una CloudWatch alarma basada en un filtro métrico de grupo de registros](#) en la Guía CloudWatch del usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que sea... <i>your-metric-name</i>	Mayor/Igual
que...	1

[CloudWatch.14] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de VPC

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.14, CIS Foundations Benchmark v1.4.4.14, NIST.800-171.r2 3.3.1, AWS NIST.800-171.r2 3.13.1, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`,
`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config Regla de: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo CloudTrail los registros a CloudWatch los registros y estableciendo los filtros de métricas y alarmas correspondientes. Puede tener más de una VPC en una cuenta y puede crear una conexión de igual nivel entre dos VPCs, lo que permite que el tráfico de red se enrute entre ellas. VPCs

CIS recomienda que cree un filtro de métricas y alarma para los cambios realizados a VPCs. La monitorización de estos cambios ayuda a garantizar que los controles de autenticación y autorización permanezcan intactos.

Para ejecutar esta comprobación, Security Hub utiliza la lógica personalizada para realizar los pasos de auditoría exactos prescritos para el control 4.14 en [CIS AWS Foundations Benchmark v1.4.0](#). Este control produce un error si no se utilizan los filtros de métricas exactos prescritos por CIS. No se pueden añadir campos ni términos adicionales a los filtros de métricas.

Note

Cuando Security Hub comprueba este control, busca los CloudTrail rastros que utiliza la cuenta actual. Estas rutas pueden ser rutas de organización que pertenezcan a otra cuenta. Las rutas multirregionales también pueden estar basadas en una Región diferente. La comprobación arroja resultados de FAILED en los siguientes casos:

- No hay ningún rastro configurado.
- Las rutas disponibles que se encuentran en la Región actual y que son propiedad de una cuenta corriente no cumplen con los requisitos de control.

La comprobación da como resultado un estado de control de NO_DATA en los siguientes casos:

- Una ruta multirregional se basa en una Región diferente. Security Hub solo puede generar resultados en la Región en la que se encuentra el rastro.
- Una ruta multirregional pertenece a una cuenta diferente. Security Hub solo puede generar resultados para la cuenta propietaria de la ruta.

Recomendamos los registros de la organización para registrar los eventos de muchas cuentas de una organización. Las rutas de organización son rutas multirregionales de forma predeterminada y solo las puede gestionar la cuenta AWS Organizations de administración de o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de NO_DATA de los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub solo genera resultados para los recursos propiedad de los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de Security Hub mediante la agregación entre regiones.

Para la alarma, la cuenta corriente debe ser propietaria del tema de Amazon SNS al que se hace referencia o debe obtener acceso al tema de Amazon SNS llamando a `ListSubscriptionsByTopic`. De lo contrario, Security Hub generará resultados de WARNING para el control.

Corrección

Para pasar este control, siga estos pasos para crear un tema de Amazon SNS, una ruta de AWS CloudTrail , un filtro de métricas y una alarma para el filtro de métricas.

1. Crear un tema de Amazon SNS Para obtener instrucciones, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Cree un tema que reciba todas las alarmas del CIS y cree al menos una suscripción al tema.
2. Cree una CloudTrail ruta que se aplique a todos. Regiones de AWS Para obtener instrucciones, consulte [Crear un registro de seguimiento](#) en la Guía del usuario de AWS CloudTrail .

Anote el nombre del grupo de CloudWatch registros de registros que asocie a la CloudTrail ruta. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulta Cómo [crear un filtro de métricas para un grupo de registros](#) en la Guía del CloudWatch usuario de Amazon. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{(\$.eventName=CreateVpc) (\$.eventName>DeleteVpc) (\$.eventName=ModifyVpcAttribute) (\$.eventName=AcceptVpcPeeringConnection) (\$.eventName=CreateVpcPeeringConnection) (\$.eventName>DeleteVpcPeeringConnection) (\$.eventName=RejectVpcPeeringConnection) (\$.eventName=AttachClassicLinkVpc) (\$.eventName=DetachClassicLinkVpc) (\$.eventName=DisableVpcClassicLink) (\$.eventName=EnableVpcClassicLink)}</code>
Espacio de nombres de métrica	LogMetrics
Valor de la métrica	1
Valor predeterminado	0

4. Crear una alarma basada en el filtro. Para obtener instrucciones, consulta Cómo [crear una CloudWatch alarma basada en un filtro métrico de grupo de registros](#) en la Guía CloudWatch del usuario de Amazon. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático

Campo	Valor
Siempre que sea... <i>your-metric-name</i>	Mayor/Igual
que...	1

[CloudWatch.15] CloudWatch las alarmas deben tener configuradas acciones específicas

Requisitos relacionados: NIST.800-53.r5 IR-4 (1), NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, NIST.800-53.r5 IR-4 (5), NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-4 (12), NIST.800-53.r5 SI-4 (5), NIST.800-171.r5 SI-4 (5), NIST.800-171.r2 3.3.4 800-171R2 3,14,6

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: AWS::CloudWatch::Alarm

AWS Config regla: [cloudwatch-alarm-action-check](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
alarmActionRequired	El control genera un resultado PASSED si el parámetro está establecido en true y la alarma tiene una acción cuando el estado de la alarma cambia a ALARM.	Booleano	No personalizable	true
insufficientDataAction	El control genera un resultado PASSED si el parámetro	Booleano	true o false	false

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
actionRequired	está establecido en <code>true</code> y la alarma tiene una acción cuando el estado de la alarma cambia a <code>INSUFFICIENT_DATA</code> .			
okActionRequired	El control genera un resultado <code>PASSED</code> si el parámetro está establecido en <code>true</code> y la alarma tiene una acción cuando el estado de la alarma cambia a <code>OK</code> .	Booleano	<code>true</code> o <code>false</code>	<code>false</code>

Este control comprueba si una CloudWatch alarma de Amazon tienen al menos una acción configurada para el `ALARM` estado. Se produce un error en el control si la alarma no tiene ninguna acción configurada para el estado `ALARM`. De manera opcional, puede incluir valores personalizados de parámetros para requerir también acciones de alarma para los estados `INSUFFICIENT_DATA` o `OK`.

Note

Security Hub evalúa este control en función de alarmas de CloudWatch métricas. Las alarmas de métricas pueden formar parte de alarmas compuestas que tienen configuradas las acciones especificadas. El control arroja resultados `FAILED` en los siguientes casos:

- Las acciones especificadas no están configuradas para una alarma de métrica.
- La alarma de métrica forma parte de una alarma compuesta que tiene configuradas las acciones especificadas.

Este control se centra en si una CloudWatch alarma tiene una acción de alarma configurada, mientras que [CloudWatch.17](#) se centra en el estado de activación de una acción de CloudWatch alarma.

Recomendamos que las acciones de CloudWatch alarma le avisen automáticamente cuando una métrica monitoreada supere el umbral definido. Las alarmas de supervisión ayudan a identificar actividades inusuales y a responder rápidamente a los problemas operativos y de seguridad cuando una alarma pasa a un estado específico. El tipo más común de acción de alarma es notificar a uno o más usuarios mediante el envío de un mensaje a un tema de Amazon Simple Notification Service (Amazon SNS).

Corrección

Para obtener información sobre las acciones que admiten las CloudWatch alarmas, consulta [Acciones de alarma](#) en la Guía del CloudWatch usuario de Amazon.

[CloudWatch.16] Los grupos de CloudWatch registros deben retenerse durante un periodo específico

Categoría: Identificar - Registro

Requisitos relacionados: NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-12

Gravedad: media

Tipo de recurso: AWS::Logs::LogGroup

AWS Config regla: [cw-loggroup-retention-period-check](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub	
minRetentionTime	Período mínimo de retención en días para los grupos de CloudWatch registros	Enum	365, 400, 545, 731, 1827, 3653	365	

Este control comprueba si un grupo de CloudWatch registros de Amazon tiene un periodo de retención de al menos la cantidad de días especificada. Se produce un error en el control si el periodo de retención es inferior a la cantidad especificada. A menos que se proporcione un valor personalizado de parámetro para el periodo de retención, Security Hub utiliza un valor predeterminado de 365 días.

CloudWatch Los registros le permite centralizar los registros de todos los sistemas, aplicaciones y servicios de que utilice, Servicios de AWS en un único servicio de gran escalabilidad. Puede utilizar CloudWatch Registros para supervisar y almacenar los archivos de registro y acceder a estos desde instancias de Amazon Elastic Compute Cloud (EC2) AWS CloudTrail,, Amazon Route 53 y otras fuentes. Conservar los registros durante al menos un año puede ayudarle a cumplir con los estándares de retención de registros.

Corrección

Para configurar los ajustes de retención de registros, consulta [Cambiar la retención de datos de registro en CloudWatch los registros](#) en la Guía del CloudWatch usuario de Amazon.

[CloudWatch.17] las acciones CloudWatch de alarma deben estar activadas

Categoría: Detectar - Servicios de detección

Requisitos relacionados: NIST.800-53.r5 SI-2 NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-4 (12)

Gravedad: alta

Tipo de recurso: `AWS::CloudWatch::Alarm`

AWS Config regla: [cloudwatch-alarm-action-enabled-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si están activadas las acciones de CloudWatch alarma (ActionEnabled debe configurarse en true). El control falla si la acción de alarma de una CloudWatch alarma está desactivada.

 Note

Security Hub evalúa este control en función de alarmas de CloudWatch métricas. Las alarmas de métricas pueden formar parte de alarmas compuestas que tienen activadas las acciones de alarma. El control arroja resultados FAILED en los siguientes casos:

- Las acciones especificadas no están configuradas para una alarma de métrica.
- La alarma de métrica forma parte de una alarma compuesta que tiene activadas las acciones de alarma.

Este control se centra en el estado de activación de una acción de CloudWatch alarma, mientras que [CloudWatch.15](#) se centra en si hay alguna ALARM acción configurada en una CloudWatch alarma.

Las acciones de alarma le avisan automáticamente cuando una métrica monitorizada está fuera del umbral definido. Si la acción de alarma está desactivada, no se ejecuta ninguna acción cuando la alarma cambia de estado y no se le avisará de los cambios en las métricas monitorizadas. Recomendamos activar las acciones de CloudWatch alarma para ayudarle a responder rápidamente a los problemas operativos y de seguridad.

Corrección

Cómo activar una acción CloudWatch de alarma (consola)

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Alarmas y, luego, Todas las alarmas.
3. Seleccione la alarma para la que desea activar las acciones.
4. En Acciones, selecciona Acciones de alarma (nuevas) y, a continuación, selecciona Habilitar.

Para obtener más información sobre la activación de las acciones de CloudWatch alarma, consulta [Acciones de alarma](#) en la Guía del CloudWatch usuario de Amazon.

Controles de Security Hub para CodeArtifact

Estos controles de Security Hub evalúan el AWS CodeArtifact servicio y los recursos.

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[CodeArtifact.1] CodeArtifact Los repositorios deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::CodeArtifact::Repository

Regla de AWS Config : tagged-codeartifact-repository (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un AWS CodeArtifact repositorio tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el repositorio no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si

no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el repositorio no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un CodeArtifact repositorio, consulte [Etiquetar un repositorio CodeArtifact en](#) la Guía del AWS CodeArtifact usuario.

Controles de Security Hub para CodeBuild

Estos controles de Security Hub evalúan el AWS CodeBuild servicio y los recursos.

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[CodeBuild.1] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales

Requisitos relacionados: PCI DSS NIST.800-53.r5 SA-3 v3.2.1/8.2.1, PCI DSS v4.0.1/8.3.2

Categoría: Proteger - Desarrollo seguro

Gravedad: crítica

Tipo de recurso: AWS::CodeBuild::Project

Regla de AWS Config : [codebuild-project-source-repo-url-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la URL del repositorio fuente de Bitbucket de un AWS CodeBuild proyecto contiene tokens de acceso personales o un nombre de usuario y una contraseña. El control falla si la URL del repositorio de origen de Bitbucket contiene tokens de acceso personal o un nombre de usuario y una contraseña.

 Note

Este control evalúa tanto la fuente principal como las fuentes secundarias de un proyecto de CodeBuild compilación. Para obtener más información acerca de los orígenes del proyecto, consulte [Multiple input sources and output artifacts sample](#) en la Guía del usuario de AWS CodeBuild .

Las credenciales de inicio de sesión no deben almacenarse o transmitirse en texto sin formato ni aparecer en la URL del repositorio de origen. En lugar de utilizar fichas de acceso personales o credenciales de inicio de sesión, debes acceder a tu proveedor de fuentes y cambiar la URL del repositorio de origen para que contenga solo la ruta a la ubicación del repositorio de Bitbucket. CodeBuild El uso de tokens de acceso personal o de credenciales de inicio de sesión podría dar lugar a la exposición involuntaria de datos o al acceso no autorizado.

Corrección

Puedes actualizar tu CodeBuild proyecto para usarlo. OAuth

Para eliminar el token de autenticación básica/(GitHub) de acceso personal de la fuente del CodeBuild proyecto

1. Abra la CodeBuild consola en <https://console.aws.amazon.com/codebuild/>.

2. Elija el proyecto de compilación que contiene tokens de acceso personales o un nombre de usuario y una contraseña.
3. En Edit (Editar), elija Source (Origen).
4. Selecciona Desconectar de GitHub /Bitbucket.
5. Selecciona Conectar mediante OAuth y, a continuación, selecciona Conectar a GitHub / Bitbucket.
6. Cuando se le solicite, elija authorize as appropriate (autorizar según corresponda).
7. Vuelva a configurar la URL de repositorio y los ajustes de la configuración adicional, según sea necesario.
8. Elija Update source (Actualizar origen).

Para obtener más información, consulta los [ejemplos basados en casos de CodeBuild uso](#) en la Guía del AWS CodeBuild usuario.

[CodeBuild.2] Las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro

Requisitos relacionados: NIST.800-53.r5 IA-5 (7), PCI DSS NIST.800-53.r5 SA-3 v3.2.1/8.2.1, PCI DSS v4.0.1/8.3.2

Categoría: Proteger - Desarrollo seguro

Gravedad: crítica

Tipo de recurso: AWS::CodeBuild::Project

Regla de AWS Config : [codebuild-project-envvar-awscred-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el proyecto contiene las variables de entorno AWS_ACCESS_KEY_ID y AWS_SECRET_ACCESS_KEY.

Las credenciales de autenticación AWS_ACCESS_KEY_ID y AWS_SECRET_ACCESS_KEY no deben almacenarse nunca en texto sin cifrar, ya que esto podría conducir a una exposición no intencionada de los datos y a un acceso no autorizado.

Corrección

[Para eliminar las variables de entorno de un proyecto, consulte Cambiar la configuración de un CodeBuild proyecto de compilación en la Guía del usuario. AWS CodeBuildAWS CodeBuild](#)

Asegúrese de que no haya nada seleccionado para las Variables de entorno.

Puede almacenar variables de entorno con valores sensibles en el almacén de AWS Systems Manager parámetros o AWS Secrets Manager , a continuación, recuperarlas de las especificaciones de compilación. Para obtener instrucciones, consulte el cuadro denominado Importante en la [sección Medio ambiente](#) de la Guía del usuario de AWS CodeBuild .

[CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-2 NIST.800-53.r5 SI-7 (6), PCI DSS v4.0.1/10.3.2

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: baja

Tipo de recurso: AWS::CodeBuild::Project

Regla de AWS Config : [codebuild-project-s3-logs-encrypted](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los registros de Amazon S3 de un AWS CodeBuild proyecto están cifrados. El control falla si se desactiva el cifrado de los registros de S3 de un CodeBuild proyecto.

El cifrado de los datos en reposo es una práctica recomendada para añadir una capa de gestión del acceso a los datos. El cifrado de los registros inactivos reduce el riesgo de que un usuario no autenticado acceda AWS a los datos almacenados en el disco. Añade otro conjunto de controles de acceso para limitar la capacidad de los usuarios no autorizados de acceder a los datos.

Corrección

Para cambiar la configuración de cifrado de los registros CodeBuild del proyecto S3, consulte [Cambiar la configuración de un proyecto de compilación AWS CodeBuild en](#) la Guía del AWS CodeBuild usuario.

[CodeBuild.4] Los entornos de los CodeBuild proyectos deben tener una duración de registro AWS Config

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), (4), NIST.800-53.r5 AC-2 (26), (9), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 Nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, Nist.800-53.r5 SI-4, Nist.800-53.r5 SI-4 (20), Nist.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::CodeBuild::Project

Regla de AWS Config : [codebuild-project-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el entorno de un CodeBuild proyecto tiene al menos una opción de registro, ya sea para S3 o para CloudWatch registros habilitados. Este control falla si un entorno de CodeBuild proyecto no tiene habilitada al menos una opción de registro.

Desde una perspectiva de seguridad, el registro es una característica importante para permitir futuros esfuerzos forenses en caso de cualquier incidente de seguridad. La correlación de las anomalías en los CodeBuild proyectos con las detecciones de amenazas puede aumentar la confianza en la precisión de esas detecciones de amenazas.

Corrección

Para obtener más información sobre cómo configurar los ajustes CodeBuild del registro del proyecto, consulte [Crear un proyecto de compilación \(consola\) en la Guía del](#) usuario. CodeBuild

[CodeBuild.5] Los entornos de CodeBuild proyectos no deberían tener habilitado el modo privilegiado

Important

Security Hub retiró este control en abril de 2024. Para obtener más información, consulte [Registro de cambios para los controles CSPM de Security Hub](#).

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2)

Categoría: Proteger > Administración de acceso seguro

Gravedad: alta

Tipo de recurso: AWS::CodeBuild::Project

Regla de AWS Config : [codebuild-project-environment-privileged-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el entorno de un AWS CodeBuild proyecto tiene el modo privilegiado activado o desactivado. El control falla si el entorno de un CodeBuild proyecto tiene habilitado el modo privilegiado.

De forma predeterminada, los contenedores Docker no permiten el acceso a ningún dispositivo. El modo privilegiado otorga acceso al contenedor Docker de un proyecto de compilación a todos los dispositivos. La configuración `privilegedMode` con un valor `true` permite que el daemon de Docker se ejecute dentro de un contenedor de Docker. El daemon de Docker escucha las solicitudes de la API de Docker y administra los objetos de Docker, como imágenes, contenedores, redes y volúmenes. Este parámetro solo debe establecerse en `true` si el proyecto de compilación se utiliza para compilar imágenes de Docker. De lo contrario, esta configuración debe estar deshabilitada para evitar el acceso no deseado a Docker APIs y al hardware subyacente del contenedor. Esta configuración de `privilegedMode` como `false` a proteger los recursos críticos contra la manipulación y la eliminación.

Corrección

Para configurar los ajustes CodeBuild del entorno del proyecto, consulte [Crear un proyecto de compilación \(consola\)](#) en la Guía del CodeBuild usuario. En la sección Entorno, no seleccione la configuración Privilegiada.

[CodeBuild.7] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::CodeBuild::ReportGroup

Regla de AWS Config : [codebuild-report-group-encrypted-at-rest](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los resultados de las pruebas de un grupo de AWS CodeBuild informes que se exportan a un bucket de Amazon Simple Storage Service (Amazon S3) están cifrados en reposo. El control falla si la exportación del grupo de informes no está cifrada en reposo.

Los datos en reposo hacen referencia a los datos que se almacenan en un almacenamiento persistente y no volátil durante cualquier periodo de tiempo. El cifrado de datos en reposo permite proteger la confidencialidad de los datos, lo que reduce el riesgo de que un usuario no autorizado pueda acceder a ellos.

Corrección

Para cifrar la exportación del grupo de informes a S3, consulte [Update a report group](#) en la Guía del usuario de AWS CodeBuild .

Controles de Security Hub para Amazon CodeGuru Profiler

Estos controles de Security Hub evalúan el servicio y los recursos de Amazon CodeGuru Profiler.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[CodeGuruProfiler.1] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::CodeGuruProfiler::ProfilingGroup`

Regla de AWS Config: `codeguruprofiler-profiling-group-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un grupo de CodeGuru perfiles de Amazon Profiler tiene etiquetas con las claves específicas definidas en el parámetro. `requiredKeyTags` El control falla si el grupo de creación de perfiles no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro. `requiredKeyTags` Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y produce un error si el grupo de creación de perfiles no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los

propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un grupo de creación de CodeGuru perfiles, consulte [Etiquetado de grupos de creación de perfiles en](#) la Guía del usuario de Amazon CodeGuru Profiler.

Controles de Security Hub para Amazon CodeGuru Reviewer

Estos controles de Security Hub evalúan el servicio y los recursos de Amazon CodeGuru Reviewer.

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[CodeGuruReviewer.1] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::CodeGuruReviewer::RepositoryAssociation

Regla de AWS Config: codegurureviewer-repository-association-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una asociación de repositorios de Amazon CodeGuru Reviewer tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si la asociación de repositorios no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si la asociación de repositorios no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws :`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una asociación de repositorios de CodeGuru Reviewer, consulte [Etiquetar una asociación de repositorios](#) en la Guía del usuario de Amazon CodeGuru Reviewer.

Controles de Security Hub para Amazon Cognito

Este AWS Security Hub control evalúa el servicio y los recursos de Amazon Cognito. Es posible que el control no esté disponible en todas las regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Cognito.1] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: `AWS::Cognito::UserPool`

Regla de AWS Config : [cognito-user-pool-advanced-security-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
SecurityMode	El modo de aplicación de la protección contra amenazas que comprueba el control.	Cadena	AUDIT, ENFORCED	ENFORCED

Este control comprueba si un grupo de usuarios de Amazon Cognito tiene activada la protección contra amenazas con el modo de aplicación configurado en pleno funcionamiento para la autenticación estándar. El control falla si el grupo de usuarios tiene desactivada la protección contra amenazas o si el modo de aplicación no está configurado para funcionar plenamente para la autenticación estándar. A menos que proporciones valores de parámetros personalizados, Security Hub utiliza el valor predeterminado de ENFORCED para el modo de aplicación establecido en función completa para la autenticación estándar.

Tras crear un grupo de usuarios de Amazon Cognito, puede activar la protección contra amenazas y personalizar las acciones que se toman en respuesta a los distintos riesgos. O bien, puede utilizar el modo de auditoría para recopilar métricas sobre los riesgos detectados sin aplicar ningún tipo de mitigación de seguridad. En el modo auditoría, Threat Protection publica las métricas en Amazon CloudWatch. Puede ver las métricas después de que Amazon Cognito genere su primer evento.

Corrección

Para obtener información sobre cómo activar la protección contra amenazas para un grupo de usuarios de Amazon Cognito, consulte [Seguridad avanzada con protección contra amenazas](#) en la Guía para desarrolladores de Amazon Cognito.

Controles de Security Hub para AWS Config

Estos controles de Security Hub evalúan el AWS Config servicio y los recursos.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Config.1] AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/2.5, CIS AWS Foundations Benchmark v1.4.0/3.5, CIS AWS Foundations Benchmark v3.0.0/3.3, NIST.800-53.r5 CM-3, NIST.800-53.r5 CM-6 (1), NIST.800-53.r5 CM-8 (2), PCI DSS v3.2.1/10.5.2, PCI DSS v3.2.1/11.5

Categoría: Identificar - Inventario

Gravedad: crítica

Tipo de recurso: AWS :: Account

AWS Config regla: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
includeConfigServiceLinkedRoleCheck	El control no evalúa si AWS Config utiliza el rol vinculado al servicio si el parámetro está establecido en. false	Booleano	true o false	true

Este control comprueba si AWS Config está habilitado en su cuenta en la actual Región de AWS, registra todos los recursos que corresponden a los controles que están habilitados en la región actual y utiliza el rol vinculado al [servicio AWS Config](#). El nombre del rol vinculado al servicio es. AWSServiceRoleForConfig Si no usa el rol vinculado al servicio y no establece el includeConfigServiceLinkedRoleCheck parámetro en false, el control fallará porque es posible que otros roles no tengan los permisos necesarios AWS Config para registrar sus recursos con precisión.

El AWS Config servicio gestiona la configuración de AWS los recursos compatibles de tu cuenta y te entrega los archivos de registro. La información registrada incluye el elemento de configuración

(AWS recurso), las relaciones entre los elementos de configuración y cualquier cambio de configuración en los recursos. Los recursos globales son recursos que están disponibles en cualquier región.

El control se evalúa de la siguiente manera:

- Si la región actual está configurada como su [región de agregación](#), el control solo produce PASSED resultados si se registran los recursos globales AWS Identity and Access Management (de IAM) (si ha activado los controles que los requieren).
- Si la región actual está configurada como una región vinculada, el control no evalúa si se registran recursos globales de IAM.
- Si la región actual no está en su agregador o si la agregación entre regiones no está configurada en la cuenta, el control solo produce resultados PASSED si se registran los recursos globales de IAM (si ha habilitado los controles que los requieren).

Los resultados del control no se ven afectados por el registro diario o continuo de los cambios en el estado de los recursos en AWS Config. Sin embargo, los resultados de este control pueden cambiar cuando se lanzan controles nuevos si se ha configurado la habilitación automática de los nuevos controles o si se cuenta con una política de configuración centralizada que habilita automáticamente los controles nuevos. En estos casos, si no registra todos los recursos, debe configurar el registro de los recursos asociados a los nuevos controles para recibir un resultado PASSED.

Los controles de seguridad de Security Hub funcionan según lo previsto solo si se habilita AWS Config en todas las regiones y se configura el registro de recursos para los controles que lo requieren.

Note

La configuración 1 requiere que AWS Config esté habilitada en todas las regiones en las que utilice Security Hub.

Como Security Hub es un servicio regional, la comprobación que se realiza con este control solo se aplica a la región actual de la cuenta.

Para admitir los controles de seguridad en recursos globales de IAM de una región, debe registrar los recursos globales de IAM en esa región. Las regiones en las que no se hayan registrado los recursos globales de IAM recibirán un resultado PASSED predeterminado por los controles que comprueban los recursos globales de IAM. Como los recursos globales de IAM son idénticos en todas las regiones de AWS, le recomendamos que registre

los recursos globales de IAM únicamente en la región de origen (si la agregación entre regiones está habilitada en su cuenta). Los recursos de IAM solo se registrarán en la región en la que esté activado el registro de recursos globales.

Los tipos de recursos de IAM registrados a nivel mundial que AWS Config admite son los usuarios, los grupos, las funciones y las políticas gestionadas por los clientes de IAM. Puede considerar desactivar los controles del concentrador de seguridad que comprueban estos tipos de recursos en las regiones en las que el registro global de recursos está desactivado. Para obtener más información, consulte [Controles sugeridos para deshabilitar en Security Hub \(CSPM\)](#).

Corrección

En la región de origen y en las regiones que no forman parte de un agregador, registre todos los recursos necesarios para los controles que están habilitados en la región actual, incluidos los recursos globales de IAM si ha habilitado los controles que requieren recursos globales de IAM.

En las regiones vinculadas, puede utilizar cualquier modo de AWS Config grabación, siempre que registre todos los recursos que correspondan a los controles que estén habilitados en la región actual. En las regiones vinculadas, si ha activado los controles que requieren el registro de los recursos globales de IAM, no recibirá ningún FAILED resultado (basta con registrar otros recursos).

El StatusReasons campo del Compliance objeto de la búsqueda puede ayudarle a determinar por qué ha fallado la búsqueda de este control. Para obtener más información, consulte [Detalles de conformidad de los resultados del control](#).

Para obtener una lista de los recursos que deben registrarse para cada control, consulte [AWS Config Recursos necesarios para los hallazgos de control](#). Para obtener información general sobre cómo habilitar AWS Config y configurar el registro de recursos, consulte [Habilitación y configuración AWS Config de Security Hub CSPM](#).

Controles de Security Hub para Amazon Connect

Estos controles de Security Hub evalúan el servicio y los recursos de Amazon Connect.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Connect.1] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::CustomerProfiles::ObjectType`

Regla de AWS Config: `customerprofiles-object-type-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un tipo de objeto de perfiles de clientes de Amazon Connect tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el tipo de objeto no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el tipo de objeto no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El

etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas, AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un tipo de objeto de perfiles de clientes, consulte [Añadir etiquetas a los recursos de Amazon Connect](#) en la Guía del administrador de Amazon Connect.

[Connect.2] Las instancias de Amazon Connect deben tener el CloudWatch registro activado

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::Connect::Instance

Regla de AWS Config : [connect-instance-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instancia de Amazon Connect está configurada para generar y almacenar registros de flujo en un grupo de CloudWatch registros de Amazon. El control falla si la

instancia de Amazon Connect no está configurada para generar y almacenar registros de flujo en un grupo de CloudWatch registros.

Los registros de flujo de Amazon Connect proporcionan detalles en tiempo real sobre los eventos de los flujos de Amazon Connect. Un flujo define la experiencia del cliente con un centro de contacto de Amazon Connect de principio a fin. De forma predeterminada, al crear una nueva instancia de Amazon Connect, se crea automáticamente un grupo de CloudWatch registros de Amazon para almacenar los registros de flujo de la instancia. Los registros de flujo pueden ayudarlo a analizar los flujos, encontrar errores y monitorear las métricas operativas. También puede configurar alertas para eventos específicos que puedan ocurrir en un flujo.

Corrección

Para obtener información sobre cómo habilitar los registros de flujo para una instancia de Amazon Connect, consulte [Habilitar los registros de flujo de Amazon Connect en un grupo de CloudWatch registros](#) de Amazon en la Guía del administrador de Amazon Connect.

Controles de Security Hub para Amazon Data Firehose

Estos controles de Security Hub evalúan el servicio y los recursos de Amazon Data Firehose.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[DataFirehose.1] Los flujos de entrega de Firehose deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 AU-3, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 AC-3, NIST.800-53.r5 SC-1 3, 8 NIST.800-53.r5 SC-2

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::KinesisFirehose::DeliveryStream

Regla de AWS Config : [kinesis-firehose-delivery-stream-encrypted](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un flujo de entrega de Amazon Data Firehose está cifrado en reposo con el cifrado del servidor. Este control falla si un flujo de entrega de Firehose no se cifra en reposo con el cifrado del servidor.

El cifrado del lado del servidor es una función de las transmisiones de entrega de Amazon Data Firehose que cifra automáticamente los datos antes de que estén en reposo mediante una clave creada en (). AWS Key Management Service AWS KMS Los datos se cifran antes de transmitirlos a la capa de almacenamiento del flujo de Data Firehose, y se descifran después de recuperarlos del almacenamiento. Esto permite cumplir con los requisitos normativos estrictos y mejorar la seguridad de sus datos.

Corrección

Para habilitar el cifrado del servidor en los flujos de entrega de Firehose, consulte [Protección de datos en Amazon Data Firehose](#) en la Guía para desarrolladores de Amazon Data Firehose.

Controles de Security Hub para AWS DataSync

Estos controles de Security Hub evalúan el AWS DataSync servicio y los recursos. Es posible que los controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[DataSync.1] DataSync las tareas deberían tener el registro activado

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::DataSync::Task

Regla de AWS Config : [datasync-task-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una AWS DataSync tarea tiene activado el registro. El control falla si la tarea no tiene habilitado el registro.

Los registros de auditoría rastrean y supervisan las actividades del sistema. Proporcionan un registro de los eventos que puede ayudarlo a detectar brechas de seguridad, investigar incidentes y cumplir

con las normativas. Los registros de auditoría también mejoran la responsabilidad y la transparencia generales de su organización.

Corrección

Para obtener información sobre cómo configurar el registro para AWS DataSync las tareas, consulte [Supervisión de las transferencias de datos con Amazon CloudWatch Logs](#) en la Guía del AWS DataSync usuario.

[DataSync.2] DataSync las tareas deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::DataSync::Task

Regla de AWS Config : [datasync-task-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Una lista de claves de etiquetas no relacionadas con el sistema que se deben asignar a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una AWS DataSync tarea tiene las claves de etiqueta especificadas en el `requiredKeyTags` parámetro. El control produce un error si la tarea no tiene ninguna clave

de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no especificas ningún valor para el `requiredKeyTags` parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si la tarea no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws:` prefijo.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarle a identificar, organizar, buscar y filtrar los recursos. También pueden ayudarte a realizar un seguimiento de las acciones y notificaciones de los propietarios de los recursos. También puedes usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas](#).

 Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están pensadas para usarse con datos privados o confidenciales.

Corrección

Para obtener información sobre cómo añadir etiquetas a una AWS DataSync tarea, consulte [Etiquetar AWS DataSync las tareas](#) en la Guía del AWS DataSync usuario.

Controles de Security Hub para Amazon Detective

Este AWS Security Hub control evalúa el servicio y los recursos de Amazon Detective. Es posible que el control no esté disponible en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Detective.1] Los gráficos de comportamiento de Detective deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Detective::Graph`

Regla de AWS Config : `tagged-detective-graph` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un gráfico de comportamiento de Amazon Detective tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el gráfico de comportamiento no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el gráfico de comportamiento no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un gráfico de comportamiento de Detective, consulte [Agregar etiquetas a un gráfico de comportamiento](#) en la Guía de administración de Amazon Detective.

Controles de Security Hub para AWS DMS

Estos controles de Security Hub evalúan el servicio y los recursos AWS Database Migration Service (AWS DMS).

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[DMS.1] Las instancias de replicación de Database Migration Service no deben ser públicas

Requisitos relacionados: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (16) NIST.800-53.r5 AC-6, (20) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.2 2.1/1.3.6, PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: AWS::DMS::ReplicationInstance

Regla de AWS Config : [dms-replication-not-public](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si las instancias de AWS DMS replicación son públicas. Para ello, examina el valor del campo `PubliclyAccessible`.

Una instancia de replicación privada tiene una dirección IP privada a la que no puede obtener acceso desde fuera de la red de replicación. Una instancia de replicación debe tener una dirección IP privada cuando las bases de datos de origen y destino estén en la misma red. La red también debe estar conectada a la VPC de la instancia de replicación mediante una VPN o un emparejamiento AWS Direct Connect de VPC. Para obtener más información sobre las instancias de replicación públicas y privadas, consulte las instancias de [Replicación públicas y privadas](#) en la Guía del usuario de AWS Database Migration Service .

También debes asegurarte de que el acceso a la configuración de tu AWS DMS instancia esté limitado únicamente a los usuarios autorizados. Para ello, restrinja los permisos de IAM de los usuarios para modificar la AWS DMS configuración y los recursos.

Corrección

No puede cambiar la configuración de acceso público de una instancia de replicación del DMS después de crearla. Para cambiar la configuración de acceso público, [elimine la instancia actual](#) y, a continuación, [vuelva a crearla](#). No seleccione la opción de Acceso público.

[DMS.2] Los certificados DMS deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::DMS::Certificate

Regla de AWS Config : `tagged-dms-certificate` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un AWS DMS certificado tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el certificado no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el certificado no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws :`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre

ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un certificado DMS, consulte [Etiquetado de recursos en AWS Database Migration Service](#) en la Guía del usuario de AWS Database Migration Service .

[DMS.3] Las suscripciones a eventos de DMS deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::DMS::EventSubscription

Regla de AWS Config : tagged-dms-eventsubscription (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si la suscripción a un AWS DMS evento tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si la suscripción a un evento no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control

solo comprueba la existencia de una clave de etiqueta y falla si la suscripción a un evento no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una inscripción a un evento, consulte [Etiquetado de recursos en AWS Database Migration Service](#) en la Guía del usuario de AWS Database Migration Service .

[DMS.4] Las instancias de replicación de DMS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::DMS::ReplicationInstance`

Regla de AWS Config : `tagged-dms-replicationinstance` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si una instancia de AWS DMS replicación tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si la instancia de replicación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si la instancia de replicación no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una instancia de replicación, consulte [Etiquetado de recursos en AWS Database Migration Service](#) en la Guía del usuario de AWS Database Migration Service .

[DMS.5] Los grupos de subredes de replicación del DMS deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::DMS::ReplicationSubnetGroup

Regla de AWS Config : tagged-dms-replicationsubnetgroup (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un grupo de subredes de AWS DMS replicación tiene etiquetas con las claves específicas definidas en el parámetro. `requiredTagKeys` El control falla si el grupo de subredes de replicación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el grupo de subredes de replicación no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un grupo de subredes de replicación, consulte [Etiquetado de recursos en AWS Database Migration Service](#) en la Guía del usuario de AWS Database Migration Service .

[DMS.6] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias

Requisitos relacionados: NIST.800-53.r5 SI-2, niST.800-53.r5 SI-2 (2), niST.800-53.r5 SI-2 (4), Nlst.800-53.r5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: media

Tipo de recurso: AWS::DMS::ReplicationInstance

Regla de AWS Config : [dms-auto-minor-version-upgrade-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la actualización automática de la versión secundaria está AWS DMS habilitada para una instancia de replicación. El control falla si la actualización automática de la versión secundaria no está habilitada para una instancia de replicación del DMS.

El DMS proporciona una actualización automática de las versiones secundarias a cada motor de replicación compatible para que pueda conservar su instancia up-to-date de replicación. Las versiones secundarias pueden introducir nuevas funciones de software, correcciones de errores, parches de seguridad y mejoras de rendimiento. Al habilitar la actualización automática de las versiones secundarias en las instancias de replicación del DMS, las actualizaciones menores se aplican automáticamente durante el período de mantenimiento o inmediatamente si se selecciona la opción Aplicar los cambios inmediatamente.

Corrección

Para habilitar la actualización automática de la versión secundaria en las instancias de replicación del DMS, consulte [Modificación de una instancia de replicación](#) en la Guía del usuario de AWS Database Migration Service .

[DMS.7] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.4.2 NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::DMS::ReplicationTask

Regla de AWS Config : [dms-replication-task-targetdb-logging](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el registro está habilitado con el nivel de gravedad mínimo `LOGGER_SEVERITY_DEFAULT` para las tareas de replicación del DMS `TARGET_APPLY` y `TARGET_LOAD`. El control falla si el registro no está habilitado para estas tareas o si el nivel de gravedad mínimo es inferior a `LOGGER_SEVERITY_DEFAULT`.

DMS utiliza Amazon CloudWatch para registrar la información durante el proceso de migración. Con la configuración de tareas de registro, puede especificar qué actividades de componentes se registran y qué cantidad de información se registra. Debe especificar el registro para las siguientes tareas:

- `TARGET_APPLY`: los datos e instrucciones de lenguaje de definición de datos (DDL) se aplican a la base de datos de destino.
- `TARGET_LOAD`: Los datos se cargan en la base de datos destino.

El registro desempeña un papel fundamental en las tareas de replicación del DMS, ya que permite la supervisión, la solución de problemas, la auditoría, el análisis del rendimiento, la detección de errores y la recuperación, así como el análisis histórico y la elaboración de informes. Ayuda a garantizar la replicación exitosa de los datos entre bases de datos y, al mismo tiempo, a mantener la integridad de los datos y el cumplimiento de los requisitos reglamentarios. Los niveles de registro que no estén fijados como `DEFAULT` suelen ser necesarios para estos componentes durante la resolución de problemas. Recomendamos mantener el nivel de registro igual que `DEFAULT` para estos componentes, a menos que se solicite específicamente cambiarlo Soporte. Un nivel de registro mínimo como `DEFAULT` garantiza que los mensajes informativos, las advertencias y los mensajes de error se escriban en los registros. Este control comprueba si el nivel de registro es al menos uno de los siguientes para las tareas de replicación anteriores: `LOGGER_SEVERITY_DEFAULT`, `LOGGER_SEVERITY_DEBUG` o `LOGGER_SEVERITY_DETAILED_DEBUG`.

Corrección

Para habilitar el registro de las tareas de replicación del DMS de la base de datos de destino, consulte [Visualización y administración de los registros de AWS DMS tareas](#) en la Guía del AWS Database Migration Service usuario.

[DMS.8] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.4.2 NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::DMS::ReplicationTask

Regla de AWS Config : [dms-replication-task-sourcedb-logging](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el registro está habilitado con el nivel de gravedad mínimo `LOGGER_SEVERITY_DEFAULT` para las tareas de replicación del DMS `SOURCE_CAPTURE` y `SOURCE_UNLOAD`. El control falla si el registro no está habilitado para estas tareas o si el nivel de gravedad mínimo es inferior a `LOGGER_SEVERITY_DEFAULT`.

DMS utiliza Amazon CloudWatch para registrar la información durante el proceso de migración. Con la configuración de tareas de registro, puede especificar qué actividades de componentes se registran y qué cantidad de información se registra. Debe especificar el registro para las siguientes tareas:

- `SOURCE_CAPTURE`: Los datos de replicación continua o captura de datos modificados (CDC) se capturan de la base de datos o el servicio de origen y se transfieren al componente de servicio de `SORTER`.
- `SOURCE_UNLOAD`: Los datos se descargan de la base de datos o del servicio de origen durante la carga completa.

El registro desempeña un papel fundamental en las tareas de replicación del DMS, ya que permite la supervisión, la solución de problemas, la auditoría, el análisis del rendimiento, la detección de errores y la recuperación, así como el análisis histórico y la elaboración de informes. Ayuda a garantizar la replicación exitosa de los datos entre bases de datos y, al mismo tiempo, a mantener

la integridad de los datos y el cumplimiento de los requisitos reglamentarios. Los niveles de registro que no estén fijados como DEFAULT suelen ser necesarios para estos componentes durante la resolución de problemas. Recomendamos mantener el nivel de registro igual que DEFAULT para estos componentes, a menos que se solicite específicamente cambiarlo Soporte. Un nivel de registro mínimo como DEFAULT garantiza que los mensajes informativos, las advertencias y los mensajes de error se escriban en los registros. Este control comprueba si el nivel de registro es al menos uno de los siguientes para las tareas de replicación anteriores: `LOGGER_SEVERITY_DEFAULT`, `LOGGER_SEVERITY_DEBUG` o `LOGGER_SEVERITY_DETAILED_DEBUG`.

Corrección

Para habilitar el registro de las tareas de replicación del DMS de la base de datos fuente, consulte [Visualización y administración de los registros de AWS DMS tareas](#) en la Guía del AWS Database Migration Service usuario.

[DMS.9] Los puntos finales del DMS deben usar SSL

Requisitos relacionados: NIST.800-53.r5 SC-1 3 NIST.800-53.r5 AC-4, 3 (NIST.800-53.r5 SC-23), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-7 (1), NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2) NIST.800-53.r5 SC-8, PCI DSS v4.0.1/4.2.1

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::DMS::Endpoint

Regla de AWS Config : [dms-endpoint-ssl-configured](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un AWS DMS punto final utiliza una conexión SSL. El control falla si el punto de conexión no usa SSL.

Las conexiones SSL y TLS proporcionan una capa de seguridad al cifrar las conexiones entre las instancias de replicación de DMS y su base de datos. El uso de certificados brinda una capa extra de seguridad al validar que la conexión se realice en una base de datos esperada. Se hace al verificar que el certificado de servidor se instale automáticamente en todas las instancias de base de datos que usted aprovisiona. Al habilitar la conexión SSL en los puntos de conexión del DMS, se protege la confidencialidad de los datos durante la migración.

Corrección

Para añadir una conexión SSL a un punto de conexión de DMS nuevo o existente, consulte [Uso de SSL de AWS Database Migration Service](#) en la Guía del usuario de AWS Database Migration Service .

[DMS.10] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM

Requisitos relacionados: NIST.800-53.r5 AC-2,, NIST.800-53.r5 AC-1 7 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-6, PCI NIST.800-53.r5 IA-2 DSS NIST.800-53.r5 IA-5 v4.0.1/7.3.1

Categoría: Proteger > Gestión del acceso seguro > Autenticación sin contraseña

Gravedad: media

Tipo de recurso: AWS::DMS::Endpoint

Regla de AWS Config : [dms-neptune-iam-authorization-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un AWS DMS punto final de una base de datos de Amazon Neptune está configurado con autorización de IAM. El control falla si el punto de conexión de DMS no tiene habilitada la autorización de IAM.

AWS Identity and Access Management (IAM) proporciona un control de acceso detallado en todas partes. AWS Con IAM, puede especificar quién puede acceder a qué servicios y recursos y en qué condiciones. Con las políticas de IAM, puede administrar los permisos del personal y sus sistemas para garantizar los permisos con privilegio mínimo. Al habilitar la autorización de IAM en AWS DMS los puntos finales de las bases de datos de Neptune, puede conceder privilegios de autorización a los usuarios de IAM mediante un rol de servicio especificado en el parámetro. ServiceAccessRoleARN

Corrección

Para habilitar la autorización de IAM en los puntos de conexión de DMS para las bases de datos de Neptune, consulte [Uso de Amazon Neptune como destino para AWS Database Migration Service](#) en la Guía del usuario de AWS Database Migration Service .

[DMS.11] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado

Requisitos relacionados: NIST.800-53.r5 AC-3,,, PCI DSS NIST.800-53.r5 AC-6 NIST.800-53.r5 IA-2 v4.0.1/7.3.1 NIST.800-53.r5 IA-5

Categoría: Proteger > Gestión del acceso seguro > Autenticación sin contraseña

Gravedad: media

Tipo de recurso: AWS::DMS::Endpoint

Regla de AWS Config : [dms-mongo-db-authentication-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un AWS DMS punto final para MongoDB está configurado con un mecanismo de autenticación. El control falla si no se estableció un tipo de autenticación para el punto de conexión.

AWS Database Migration Service admite dos métodos de autenticación para MongoDB: MONGODB-CR para MongoDB versión 2.x y SCRAM-SHA-1 para MongoDB versión 3.x o posterior. Estos métodos de autenticación se utilizan para autenticar y cifrar las contraseñas de MongoDB si los usuarios desean utilizarlas para acceder a las bases de datos. La autenticación en los AWS DMS puntos finales garantiza que solo los usuarios autorizados puedan acceder a los datos que se migran entre bases de datos y modificarlos. Sin la autenticación adecuada, los usuarios no autorizados pueden acceder a datos confidenciales durante el proceso de migración. Esto puede provocar filtraciones de datos, pérdida de datos u otros incidentes de seguridad.

Corrección

Para habilitar un mecanismo de autenticación en los puntos de conexión de DMS para MongoDB, consulte [Uso de MongoDB como origen en AWS DMS](#) en la Guía del usuario de AWS Database Migration Service .

[DMS.12] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado

Requisitos relacionados: NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-1 3, PCI DSS v4.0.1/4.2.1

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::DMS::Endpoint

Regla de AWS Config : [dms-redis-tls-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un AWS DMS punto final para Redis OSS está configurado con una conexión TLS. El control falla si el punto de conexión no tiene habilitado el TLS.

El TLS proporciona end-to-end seguridad cuando los datos se envían entre aplicaciones o bases de datos a través de Internet. Al configurar el cifrado SSL para su punto de conexión de DMS, permite la comunicación cifrada entre las bases de datos de origen y destino durante el proceso de migración. Esto ayuda a evitar el espionaje y la interceptación de datos confidenciales por parte de actores malintencionados. Sin el cifrado SSL, se puede acceder a los datos confidenciales, lo que provoca filtraciones de datos, pérdida de datos u otros incidentes de seguridad.

Corrección

Para habilitar una conexión TLS en los puntos de conexión de DMS para Redis, consulte [Uso de Redis como destino para AWS Database Migration Service](#) en la Guía del usuario de AWS Database Migration Service .

Controles de Security Hub para Amazon DocumentDB

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon DocumentDB (compatible con MongoDB). Es posible que los controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [docdb-cluster-encrypted](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de Amazon DocumentDB está cifrado en reposo. El control falla si un clúster de Amazon DocumentDB no está cifrado en reposo.

Los datos en reposo se refieren a cualquier dato que se almacene en un almacenamiento persistente y no volátil durante cualquier período de tiempo. El cifrado le ayuda a proteger la confidencialidad de dichos datos, reduciendo el riesgo de que un usuario no autorizado acceda a ellos. Los datos de los clústeres de Amazon DocumentDB deben cifrarse en reposo para ofrecer un nivel de seguridad adicional. Amazon DocumentDB utiliza el estándar de cifrado avanzado de 256 bits (AES-256) para cifrar los datos mediante claves de cifrado almacenadas en AWS Key Management Service (AWS KMS).

Corrección

Puede habilitar el cifrado en reposo al crear un clúster de Amazon DocumentDB. No se puede cambiar la configuración de cifrado después de crear un clúster. Para obtener más información, consulte [Habilitar el cifrado en reposo para un clúster de Amazon DocumentDB](#) en la Guía para desarrolladores de Amazon DocumentDB.

[DocumentDb.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado

Requisitos relacionados: NIST.800-53.r5 SI-12, PCI DSS v4.0.1/3.2.1

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [docdb-cluster-backup-retention-check](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub	
minimumBackupRetentionPeriod	El periodo mínimo de retención de copias de seguridad en días	Entero	De 7 a 35	7	

Este control comprueba si un clúster de Amazon DocumentDB tiene un periodo de retención de copias de seguridad superior o igual al periodo especificado. Se produce un error en el control si el periodo de retención de copia de seguridad es inferior al periodo especificado. A menos que se proporcione un valor personalizado de parámetro para el periodo de retención de copia de seguridad, Security Hub utiliza un valor predeterminado de 7 días.

Las copias de seguridad le ayudan a recuperarse más rápidamente de un incidente de seguridad y a reforzar la resiliencia de sus sistemas. Al automatizar las copias de seguridad de los clústeres de Amazon DocumentDB, podrá restaurar los sistemas en un momento determinado y minimizar el tiempo de inactividad y la pérdida de datos. En Amazon DocumentDB, los clústeres tienen un periodo predeterminado de retención de copia de seguridad de 1 día. Debe aumentarse a un valor de entre 7 y 35 días para superar este control.

Corrección

Para cambiar el período de retención de copias de seguridad de sus clústeres de Amazon DocumentDB, consulte [Modificación de un clúster de Amazon DocumentDB](#) en la Guía para desarrolladores de Amazon DocumentDB. En Copia de seguridad, elija el periodo de retención de copia de seguridad.

[DocumentDb.3] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas

Requisitos relacionados: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21), (11) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (16), (20) NIST.800-53.r5 AC-6 NIST.800-53.r5

SC-7, NIST.800-53.r5 SC-7 (21), (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS NIST.800-53.r5 SC-7 v4.0.1/1.4.4 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: AWS::RDS::DBClusterSnapshot

Regla de AWS Config : [docdb-cluster-snapshot-public-prohibited](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instantánea de clúster manual de Amazon DocumentDB es pública. El control falla si la instantánea manual del clúster es pública.

Una instantánea manual de un clúster de Amazon DocumentDB no debe ser pública a menos que se pretenda. Si comparte una instantánea manual sin cifrar públicamente, la instantánea estará disponible para todo Cuentas de AWS. Las instantáneas públicas pueden provocar una exposición no intencionada de los datos.

Note

Este control evalúa las instantáneas de clúster manuales. No se pueden compartir instantáneas automatizadas de un clúster de Amazon DocumentDB. Sin embargo, puede crear una instantánea manual copiando la instantánea automatizada y compartiéndola después.

Corrección

Para eliminar el acceso público a las instantáneas de clústeres manuales de Amazon DocumentDB, consulte [Compartir una instantánea](#) en la Guía para desarrolladores de Amazon DocumentDB. Mediante programación, puede utilizar la operación Amazon DocumentDB de `modify-db-snapshot-attribute`. Establecer `attribute-name` en `restore` y `values-to-remove` en `all`.

[DocumentDb.4] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), (9), NIST.800-53.r5 AC-6 Nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, Nist.800-53.r5 SI-4 (20), Nist.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.3.3

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [docdb-cluster-audit-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de Amazon DocumentDB publica registros de auditoría en Amazon CloudWatch Logs. El control falla si el clúster no publica los registros de auditoría en CloudWatch Logs.

Amazon DocumentDB (con compatibilidad con MongoDB) le permite auditar eventos que se realizaron en su clúster. Los intentos de autenticación correctos e incorrectos, la eliminación de una colección en una base de datos o la creación de un índice son algunos ejemplos de eventos registrados. De forma predeterminada, la auditoría está deshabilitada en Amazon DocumentDB y requiere que tome medidas para habilitarla.

Corrección

Para publicar los registros de auditoría de Amazon DocumentDB en Logs, consulte [Habilitar la auditoría](#) en la Guía para CloudWatch desarrolladores de Amazon DocumentDB.

[DocumentDb.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [docdb-cluster-deletion-protection-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de Amazon DocumentDB tiene habilitada la protección contra eliminación. El control falla si el clúster no tiene habilitada la protección contra eliminación.

La activación de la protección contra la eliminación de clústeres ofrece un nivel adicional de protección contra la eliminación accidental de la base de datos o la eliminación por parte de un usuario no autorizado. No se puede eliminar un clúster de Amazon DocumentDB mientras esté habilitada la protección contra eliminación. Primero debe deshabilitar la protección contra la eliminación para que la solicitud de eliminación se pueda realizar correctamente. La protección contra eliminación se habilita de forma predeterminada cuando crea un clúster mediante la consola de Amazon DocumentDB.

Corrección

Para habilitar la protección contra la eliminación de un clúster de Amazon DocumentDB existente, consulte [Modificación de un clúster de Amazon DocumentDB](#) en la Guía para desarrolladores de Amazon DocumentDB. En la sección Modificar el clúster, seleccione Habilitar la Protección contra la eliminación.

[DocumentDb.6] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [docdb-cluster-encrypted-in-transit](#)

Tipo de programa: Periódico

Parámetro **excludeTlsParameters**: disabled, enabled (no personalizables)

Este control comprueba si un clúster de Amazon DocumentDB requiere TLS para las conexiones al clúster. El control falla si el grupo de parámetros del clúster asociado al clúster no está sincronizado o si el parámetro del clúster de TLS está establecido en `o. disabled` `enabled`

Puede usar TLS para cifrar la conexión entre una aplicación y un clúster de Amazon DocumentDB. El uso de TLS puede ayudar a evitar que los datos sean interceptados mientras los datos están en tránsito entre una aplicación y un clúster de Amazon DocumentDB. El cifrado en tránsito de un clúster de Amazon DocumentDB se administra mediante el parámetro TLS del grupo de parámetros del clúster asociado al clúster. Cuando se habilita el cifrado en tránsito, se requieren conexiones seguras con TLS para conectarse al clúster. Se recomienda utilizar los siguientes parámetros de TLS: `tls1.2+`, `ytls1.3+`, `fips-140-3`

Corrección

Para obtener información sobre cómo cambiar la configuración de TLS de un clúster de Amazon DocumentDB, [consulte Cifrado de datos en tránsito en la](#) Guía para desarrolladores de Amazon DocumentDB.

Controles de Security Hub para DynamoDB

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon DynamoDB. Es posible que los controles no estén disponibles en todas las regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[DynamoDB.1] Las tablas de DynamoDB deberían escalar automáticamente la capacidad en función de la demanda

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::DynamoDB::Table

Regla de AWS Config : [dynamodb-autoscaling-enabled](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados válidos	Valor predeterminado de Security Hub
<code>minProvisionedReadCapacity</code>	Número mínimo de unidades de capacidad de lectura aprovisionadas para el escalado automático de DynamoDB	Entero	De 1 a 40000	Sin valor predeterminado
<code>targetReadUtilization</code>	Porcentaje de uso objetivo de capacidad de lectura	Entero	De 20 a 90	Sin valor predeterminado
<code>minProvisionedWriteCapacity</code>	Número mínimo de unidades de capacidad de escritura aprovisionadas para el escalado automático de DynamoDB	Entero	De 1 a 40000	Sin valor predeterminado
<code>targetWriteUtilization</code>	Porcentaje de uso objetivo de capacidad de escritura	Entero	De 20 a 90	Sin valor predeterminado

Este control comprueba si una tabla de Amazon DynamoDB puede escalar su capacidad de lectura y escritura según sea necesario. Se produce un error en el control si la tabla utiliza el modo de capacidad bajo demanda o el modo aprovisionado con el escalado automático configurado. De manera predeterminada, este control solo requiere que se configure uno de estos modos, independientemente de los niveles específicos de la capacidad de lectura o escritura. De manera opcional, puede proporcionar valores personalizados de parámetros para requerir niveles específicos de la capacidad de lectura y escritura o de utilización objetivo.

Escalar la capacidad en función de la demanda evita limitar las excepciones, lo que ayuda a mantener la disponibilidad de las aplicaciones. Las tablas de DynamoDB que usan el modo de capacidad bajo demanda solo están limitadas por las cuotas predeterminadas de rendimiento de las tablas de DynamoDB. Para aumentar estas cuotas, puede presentar una solicitud de asistencia en.

Soporte Las tablas de DynamoDB que usan el modo aprovisionado con escalado automático ajustan la capacidad de rendimiento aprovisionada de forma dinámica de acuerdo con los patrones de tráfico. Para obtener más información acerca de la limitación de solicitudes de DynamoDB, consulte [Limitación controlada de solicitudes y capacidad de ampliación](#) en la Guía para desarrolladores de Amazon DynamoDB.

Corrección

Para habilitar el escalado automático de DynamoDB en tablas existentes en el modo de capacidad, consulte [Habilitación de la función Auto Scaling de DynamoDB en tablas existentes](#) en la Guía para desarrolladores de Amazon DynamoDB.

[DynamoDB.2] Las tablas de DynamoDB deben tener habilitada la recuperación point-in-time

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: media

Tipo de recurso: AWS::DynamoDB::Table

Regla de AWS Config : [dynamodb-pitr-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la point-in-time recuperación (PITR) está habilitada para una tabla de Amazon DynamoDB.

Las copias de seguridad le ayudan a recuperarse más rápidamente de un incidente de seguridad. También refuerzan la resiliencia de sus sistemas. La recuperación de point-in-time DynamoDB automatiza las copias de seguridad de las tablas de DynamoDB. Reduce el tiempo de recuperación tras operaciones de borrado o escritura accidentales. Las tablas de DynamoDB que tienen PITR habilitada se pueden restaurar a cualquier momento de los últimos 35 días.

Corrección

Para restaurar una tabla de DynamoDB a un punto en el tiempo, consulte [Restauración de una tabla de DynamoDB a un punto en el tiempo](#) en la Guía para desarrolladores de Amazon DynamoDB.

[DynamoDB.3] Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::DAX::Cluster

Regla de AWS Config : [dax-encryption-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un clúster de Acelerador de Amazon DynamoDB (DAX) está cifrado en reposo. El control lanza un error si un clúster de DAX no está cifrado en reposo.

El cifrado de los datos en reposo reduce el riesgo de que un usuario no autenticado acceda a los datos almacenados en el disco. AWS El cifrado añade otro conjunto de controles de acceso para limitar la capacidad de los usuarios no autorizados de acceder a los datos. Por ejemplo, se requieren permisos de API para descifrar los datos antes de que puedan leerse.

Corrección

No puede habilitar o deshabilitar el cifrado en reposo después de haber creado un clúster. Debe volver a crear el clúster para habilitar el cifrado en reposo. Para obtener instrucciones detalladas sobre cómo crear un clúster de DAX con el cifrado en reposo activado, consulte [Habilitar el cifrado en reposo mediante la AWS Management Console](#) en la Guía para desarrolladores de Amazon DynamoDB.

[DynamoDB.4] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: media

Tipo de recurso: AWS::DynamoDB::Table

AWS Config regla: [dynamodb-resources-protected-by-backup-plan](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
backupVaultLockCheck	El control produce un PASSED resultado si el parámetro está establecido en AWS Backup Vault Lock true y el recurso lo utiliza.	Booleano	true o false	Sin valor predeterminado

Este control evalúa si una tabla de Amazon DynamoDB en estado ACTIVE está cubierta por un plan de copias de seguridad. Se produce un error en el control si la tabla de DynamoDB no está cubierta por un plan de copias de seguridad. Si establece el backupVaultLockCheck parámetro en un valor igual a true, el control solo pasa si la tabla de DynamoDB está guardada en AWS Backup un almacén cerrado.

AWS Backup es un servicio de copias de seguridad totalmente gestionado que le ayuda a centralizar y automatizar las copias de seguridad de todos los datos. Servicios de AWS Con AWS Backup, puede crear planes de respaldo que definan sus requisitos de respaldo, como la frecuencia con la que debe realizar copias de seguridad de sus datos y cuánto tiempo debe conservarlas. La inclusión de tablas de DynamoDB en sus planes de copia de seguridad le ayuda a proteger sus datos de pérdidas o eliminaciones involuntarias.

Corrección

Para agregar una tabla de DynamoDB a AWS Backup un plan de respaldo, [consulte Asignación de recursos a un plan de respaldo en la Guía para desarrolladores](#). AWS Backup

[DynamoDB.5] Las tablas de DynamoDB deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::DynamoDB::Table

Regla de AWS Config : tagged-dynamodb-table (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si una tabla de Amazon DynamoDB tiene etiquetas con claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la tabla no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la tabla no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control

de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una tabla de DynamoDB, consulte [Etiquetado de recursos en DynamoDB](#) en la Guía para desarrolladores de Amazon DynamoDB.

[DynamoDB.6] Las tablas de DynamoDB deben tener la protección contra eliminación habilitada

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Gravedad: media

Tipo de recurso: AWS::DynamoDB::Table

AWS Config regla: [dynamodb-table-deletion-protection-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una tabla de Amazon DynamoDB tiene habilitada la protección contra eliminación. Se produce un error en el control si una tabla DynamoDB no tiene habilitada la protección contra eliminación.

Puede proteger una tabla de DynamoDB contra la eliminación accidental con la propiedad de protección contra la eliminación. Habilitar esta propiedad para las tablas ayuda a garantizar que los administradores no eliminen las tablas accidentalmente durante las operaciones habituales de administración. De este modo, evita que se interrumpan las operaciones comerciales normales.

Corrección

Para habilitar la protección contra eliminación de una tabla de DynamoDB, consulte [Uso de la protección contra eliminación](#) en la Guía para desarrolladores de Amazon DynamoDB.

[DynamoDB.7] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito

Requisitos relacionados: NIST.800-53.r5 AC-1 7, 3, NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-2 3 NIST.800-53.r5 SC-8, PCI DSS v4.0.1/4.2.1

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::DAX::Cluster

Regla de AWS Config : [dax-tls-endpoint-encryption](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un clúster de Acelerador de Amazon DynamoDB (DAX) está cifrado en tránsito, con el tipo de cifrado de punto de conexión establecido en TLS. El control lanza un error si el clúster de DAX no está cifrado en tránsito.

El HTTPS (TLS) se puede utilizar para evitar que posibles atacantes utilicen ataques similares para espiar person-in-the-middle o manipular el tráfico de la red. Solo debe permitir que conexiones cifradas pasen por TLS para acceder a los clústeres de DAX. Sin embargo, el cifrado de los datos en tránsito puede afectar el rendimiento. Debe probar su aplicación con cifrado para comprender el perfil de rendimiento y el impacto de TLS.

Corrección

No se puede cambiar la configuración de cifrado de TLS después de crear un clúster de DAX. Para cifrar un clúster de DAX existente, cree un nuevo clúster con el cifrado en tránsito habilitado, traslade

el tráfico de la aplicación hacia él y, a continuación, elimine el clúster anterior. Para obtener más información, consulte [Uso de la protección contra eliminación](#) en la Guía para desarrolladores de Amazon DynamoDB.

Controles de Security Hub para Amazon EC2

Estos AWS Security Hub controles de evalúan el servicio y los recursos de Amazon Elastic Compute Cloud (Amazon EC2). Es posible que los controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[EC2.1] Las instantáneas de Amazon EBS no se deben poder restaurar públicamente

Requisitos relacionados: PCI DSS v3.2.1/1.1.1/1.2.1, PCI DSS v3.2.1/1.1.1/1.3.4, PCI DSS v3.2.1/7.2.1/7.2.1, (3), (3), NIST.800-53.r5 AC-2 (3), (2), (16) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (16) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (20) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (21) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: AWS :: Account

Regla de AWS Config : [ebs-snapshot-public-restorable-check](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si las instantáneas de Amazon Elastic Block Store no son públicas. El control falla si cualquier persona puede restaurar las instantáneas de Amazon EBS.

Las instantáneas de EBS se utilizan para hacer una copia de seguridad de los datos de sus volúmenes de EBS en Amazon S3 en un momento específico. Puede utilizar las instantáneas para restaurar estados anteriores de volúmenes de EBS. Rara vez es aceptable compartir una instantánea con el público. Por lo general, la decisión de compartir una instantánea públicamente se toma por error o sin una comprensión completa de las consecuencias. Esta comprobación ayuda a garantizar que todos esos intercambios se planificaron y son intencionados.

Corrección

Para hacer que una instantánea pública de EBS sea privada, consulte [Compartir una instantánea](#) en la Guía del EC2 usuario de Amazon. En Acciones, Modificar permisos, seleccione Privado.

[EC22] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente

Requisitos relacionados: PCI DSS v3.2.1/1.2.0/1.2.0/1.4.0/2.1, NININIS v3.2.1/2.1, NIS Benchmark v1.2.0/4.3, NIS Foundations Benchmark v1.4.0/5.3, CIS AWS Foundations Benchmark v3.0.0/5.4, (AWS 21), (11), (16), (16), (AWS 21) NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: AWS::EC2::SecurityGroup

Regla de AWS Config : [vpc-default-security-group-closed](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba que el grupo de seguridad predeterminado de una VPC permita el tráfico entrante o saliente. El control falla si el grupo de seguridad permite el tráfico entrante o saliente.

Las reglas del [grupo de seguridad predeterminado](#) permiten todo el tráfico saliente y entrante de las interfaces de red (y de sus instancias asociadas) asignadas al mismo grupo de seguridad. Le recomendamos que no utilice el grupo de seguridad predeterminado. Dado que el grupo de seguridad predeterminado no se puede eliminar, debería cambiar la configuración de reglas de grupo de seguridad predeterminada para restringir el tráfico entrante y saliente. Esto evita el tráfico no deseado si el grupo de seguridad predeterminado se configura accidentalmente para recursos como EC2 instancias.

Corrección

Para solucionar este problema, comience por crear nuevos grupos de seguridad con privilegios mínimos. Para obtener instrucciones, consulte [Crear un grupo de seguridad](#) en la Guía del usuario

de Amazon VPC. A continuación, asigne los nuevos grupos de seguridad a sus EC2 instancias. Para obtener instrucciones, consulta [Cambiar el grupo de seguridad de una instancia](#) en la Guía del EC2 usuario de Amazon.

Tras asignar los nuevos grupos de seguridad a sus recursos, elimine todas las reglas de entrada y salida de los grupos de seguridad predeterminados. Para conocer las instrucciones, consulte [Configuración de las reglas de un grupo de seguridad](#) en la Guía del usuario de Amazon VPC.

[EC2.3] Los volúmenes de Amazon EBS asociados deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::EC2::Volume

Regla de AWS Config : [encrypted-volumes](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los volúmenes de EBS asociados están cifrados. Para superar esta comprobación, los volúmenes de EBS deben tener el estado de uso y estar cifrados. Si el volumen de EBS no está asociado, entonces no estará en el alcance de esta comprobación.

Para obtener una capa adicional de seguridad de la información confidencial en volúmenes de EBS, debe habilitar el cifrado de EBS en reposo. Amazon EBS ofrece una solución de cifrado sencilla para los recursos de EBS que no precisa que cree, mantenga y proteja su propia infraestructura de administración de claves. Utiliza claves CMK al crear volúmenes cifrados e instantáneas.

Para obtener más información sobre el cifrado de Amazon EBS, consulte el cifrado de [Amazon EBS](#) en la Guía EC2 del usuario de Amazon.

Corrección

No existe una forma directa para cifrar un volumen o una instantánea sin cifrar existente. Solo puede cifrar un nuevo volumen o instantánea al crearlo.

Si ha habilitado el cifrado de forma predeterminada, Amazon EBS cifra el nuevo volumen o la instantánea resultante utilizando la clave predeterminada para el cifrado de Amazon EBS. Aunque no haya habilitado el cifrado de forma predeterminada, puede habilitarlo al crear un volumen o una instantánea individuales. En ambos casos, puede anular la clave predeterminada para el cifrado de Amazon EBS y elegir una clave administrada por el cliente simétrica.

Para obtener más información, consulte [Crear un volumen de Amazon EBS](#) y [Copiar una instantánea de Amazon EBS](#) en la Guía EC2 del usuario de Amazon.

[EC24] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoría: Identificar - Inventario

Gravedad: media

Tipo de recurso: AWS::EC2::Instance

Regla de AWS Config : [ec2-stopped-instance](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
AllowedDays	Cantidad de días que se permite que la EC2 instancia permanezca detenida antes de generar un resultado con errores.	Entero	De 1 a 365	30

Este control comprueba si una EC2 instancia de Amazon ha estado detenida durante más días de lo permitido. Se produce un error en el control si una EC2 instancia se detiene durante más tiempo

que el máximo permitido. A menos que se proporcione un valor personalizado de parámetro para el periodo máximo permitido, Security Hub utiliza un valor predeterminado de 30 días.

Cuando una EC2 instancia no se ha ejecutado durante un periodo significativo, se crea un riesgo de seguridad porque la instancia no se mantiene de forma activa (se analiza, se le aplican parches o se actualiza). Si se lanza más adelante, la falta de un mantenimiento adecuado podría provocar problemas inesperados en su AWS entorno. Para mantener segura una EC2 instancia a lo largo del tiempo en un estado inactivo, iníciela periódicamente para realizar tareas de mantenimiento y, a continuación, deténgala después del mantenimiento. Lo ideal es que se tratara de un proceso automatizado.

Corrección

Para terminar una EC2 instancia inactiva, consulta [Terminar una instancia](#) en la Guía del EC2 usuario de Amazon.

[EC2.6] El registro de flujos de VPC debe estar habilitado en todos VPCs

Requisitos relacionados: AWS NIST.800-53.0/2.9, NIST.800-53.r5 SI-7 (8), NIST.800-171.0/3.7, NIST.800-53.r5 SI-7 NIST.800-53.r5 AC-4 (8) PCI AWS DSS v3.2.1/10.3.4 NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, PCI DSS v3.2.1/10.3.1/10.3.1/10.3.6 AWS

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS : : EC2 : : VPC

Regla de AWS Config : [vpc-flow-logs-enabled](#)

Tipo de programa: Periódico

Parámetros:

- `trafficType`: REJECT (no personalizable)

Este control comprueba si se encuentran los registros de flujo de Amazon VPC y si están habilitados para VPCs. El tipo de tráfico se ha establecido como `Reject`. Se produce un error en el control si los registros de flujo de VPC no están habilitados en su cuenta.

 Note

Este control no comprueba si los registros de flujo de Amazon VPC están habilitados a través de Amazon Security Lake para la Cuenta de AWS.

Con la característica de VPC Flow Logs, puede utilizar los registros de flujo de la VPC para capturar información sobre el tráfico de direcciones IP entrante y saliente de las interfaces de red de su VPC. Una vez creado un registro del flujo, puede verlo y recuperar sus datos en CloudWatch Registros. Para reducir los costos, también puede enviar los registros de flujo a Amazon S3.

Security Hub recomienda que habilite el registro de flujo para rechazos de paquetes VPCs. Los registros de flujo proporcionan visibilidad del tráfico de red que atraviesa la VPC y pueden detectar tráfico anómalo o brindar información durante los flujos de trabajo de seguridad.

De forma predeterminada, el registro incluye valores para los distintos componentes del flujo de dirección IP, incluido el origen, el destino y el protocolo. Para obtener más información y descripciones de los campos de registro, consulte [Registros de flujo de VPC](#) en la Guía del usuario de Amazon VPC.

Corrección

Para crear un registro de flujo de VPC, consulte [Crear un registro de flujo](#) en la Guía del usuario de Amazon VPC. Tras abrir la consola de Amazon VPC, elija Su. VPCs En Filtro, elija Rechazar o Todos.

[EC2.7] El cifrado predeterminado de EBS debe estar activado

Requisitos relacionados: AWS NIST.800-53.0/2.0/2.0/2.0/2.2.1, NIST.800-53.0/2.2.1, NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8 (1), NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 SI-7 (6), NIST.800-53.r5 SC-2 NIST.800-53.r5 SI-7 (6) AWS NIST.800-53.r5 SC-7

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS :: Account

Regla de AWS Config : [ec2-ebs-encryption-by-default](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el cifrado a nivel de cuenta está habilitado de forma predeterminada para los volúmenes de Amazon Elastic Block Store (Amazon EBS). Se produce un error en el control si el cifrado a nivel de cuenta no está habilitado para los volúmenes de EBS.

Cuando el cifrado está activado en su cuenta, los volúmenes de Amazon EBS y las copias instantáneas se cifran en reposo. Esto agrega una capa adicional de protección para sus datos. Para obtener más información, consulte [Cifrado predeterminado](#) en la Guía del EC2 usuario de Amazon.

Corrección

Para configurar el cifrado predeterminado para los volúmenes de Amazon EBS, consulte [Cifrado predeterminado](#) en la Guía del EC2 usuario de Amazon.

[EC2.8] EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancias IMDSv2

Requisitos relacionados: NIS Benchmark AWS v3.0.0/5.6, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, PCI DSS v4.0.1/2.0/2.0/2.2.6 NIST.800-53.r5 AC-6

Categoría: Proteger > Seguridad de red

Gravedad: alta

Tipo de recurso: AWS::EC2::Instance

Regla de AWS Config : [ec2-imdsv2-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba EC2 si la versión de metadatos de la instancia está configurada con la versión 2 (IMDSv2). El control pasa si HttpTokens está configurado como obligatorio para IMDSv2. El control tiene errores si HttpTokens está configurado como optional,

Utiliza metadatos de instancia para configurar o administrar la instancia en ejecución. El IMDS proporciona acceso a credenciales temporales que se rotan con frecuencia. Estas credenciales eliminan la necesidad de codificar o distribuir credenciales confidenciales a las instancias de forma

manual o programática. El IMDS se conecta localmente a todas las EC2 instancias. Se ejecuta en una dirección IP de «enlace local» de 169.254.169.254. Solo el software que se ejecuta en la instancia puede acceder a esta dirección IP.

La versión 2 del IMDS añade nuevas protecciones para los siguientes tipos de vulnerabilidades. Estas vulnerabilidades podrían utilizarse para intentar acceder al IMDS.

- Abra firewalls de aplicaciones de sitios web
- Abra proxies inversos
- Vulnerabilidades de falsificación de solicitudes del servidor (SSRF)
- Firewalls de capa 3 abiertos y traducción de direcciones de red (NAT)

Security Hub recomienda configurar EC2 las instancias con IMDSv2.

Corrección

Para configurar EC2 instancias con IMDSv2, consulte [Ruta recomendada para requerir IMDSv2](#) en la Guía del EC2 usuario de Amazon.

[EC2.9] EC2 Las instancias de Amazon no deben tener una dirección pública IPv4

Requisitos relacionados: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: AWS::EC2::Instance

Regla de AWS Config : [ec2-instance-no-public-ip](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si EC2 las instancias tienen una dirección IP pública. Se produce un error en el control si el `publicIp` campo está presente en el elemento de configuración de la EC2 instancia. Este control se aplica únicamente a IPv4 las direcciones.

Una IPv4 dirección pública es una dirección IP a la que se puede tener acceso desde Internet. Si lanza la instancia con una dirección IP pública, se puede obtener acceso a la EC2 instancia desde Internet. Una IPv4 dirección privada es una dirección IP a la que no se puede obtener acceso desde Internet. Puede utilizar IPv4 direcciones privadas para la comunicación entre EC2 instancias de la misma VPC o en la red privada conectada.

IPv6 Las direcciones son únicas de forma global y, por lo tanto, están disponibles a través de Internet. De forma predeterminada, todas las subredes tienen el atributo de IPv6 direcciones configurado como falso. Para obtener más información IPv6, consulte el [direccionamiento IP en su VPC](#) en la Guía del usuario de Amazon VPC.

Si tiene un caso de uso legítimo para mantener las EC2 instancias con direcciones IP públicas, puede ocultar los resultados de este control. Para obtener más información sobre las opciones de arquitectura front-end, consulte el [Blog de AWS arquitectura](#) de o la [serie de AWS videos de This Is My Architecture](#).

Corrección

Utilice una VPC no predeterminada para que no se le asigne a su instancia una dirección IP pública de forma predeterminada.

Cuando se lanza una EC2 instancia en una VPC predeterminada, se le asigna una dirección IP pública. Al lanzar una EC2 instancia en una VPC no predeterminada, la configuración de subred determina si recibe una dirección IP pública. La subred tiene un atributo para determinar si EC2 las instancias nuevas de la subred reciben una dirección IP pública del grupo de IPv4 direcciones públicas.

Puede desvincular una dirección IP pública asignada de manera automática de su instancia. EC2 Para obtener más información, consulta [IPv4 Direcciones públicas y nombres de host DNS externos](#) en la Guía del EC2 usuario de Amazon.

[EC2.10] Amazon EC2 debe configurarse para utilizar los puntos de enlace de VPC que se crean para el servicio de Amazon EC2

Requisitos relacionados: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (16) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), (3), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 Nist.800-171.r2 NIST.800-53.r5 SC-7 3.1.3, Nist.800-171.r2 3.13.1

Categoría: Proteger > Configuración de red segura > Acceso privado a la API

Gravedad: media

Tipo de recurso: AWS::EC2::VPC

Regla de AWS Config : [service-vpc-endpoint-enabled](#)

Tipo de programa: Periódico

Parámetros:

- `serviceName: ec2` (no personalizable)

Este control comprueba si se ha creado un punto de conexión de servicio para Amazon EC2 para cada VPC. Se produce un error en el control si una VPC no tiene un punto de conexión de VPC creado para el servicio Amazon. EC2

Este control evalúa los recursos en una sola cuenta. No puede describir los recursos que están fuera de la cuenta. Dado que AWS Config y Security Hub no realiza comprobaciones entre cuentas, verá FAILED resultados VPCs que se comparten entre cuentas. Security Hub recomienda que suprima estos resultados establecidos como FAILED.

Para mejorar la posición de seguridad de su VPC, puede configurar Amazon EC2 para que utilice un punto de enlace de VPC de interfaz. Los puntos de enlace de la interfaz tienen tecnología AWS PrivateLink, que le permite obtener acceso a las operaciones de la EC2 API de Amazon de forma privada. Restringe todo el tráfico de red entre su VPC y Amazon a la red de EC2 Amazon. Dado que los puntos de conexión solo se admiten dentro de la misma región, no se puede crear un punto de conexión entre una VPC y un servicio de otra región. Esto evita las llamadas no deseadas a la EC2 API de Amazon a otras regiones.

Para obtener más información sobre la creación de puntos de enlace de VPC para Amazon, EC2 consulte [Amazon y puntos de enlace de VPC de EC2 interfaz en la Guía del usuario](#) de Amazon. EC2

Corrección

Para crear un punto de enlace de interfaz para Amazon EC2 desde la consola de Amazon VPC, consulte [Crear un punto de enlace de VPC](#) en la guía.AWS PrivateLink Para el nombre del servicio, elija `com.amazonaws.region.ec2`.

También puede crear y asociar una política de punto de conexión a su punto de conexión de VPC para controlar el acceso a la API de Amazon EC2 . Para obtener instrucciones sobre cómo crear una política de puntos de conexión de VPC, consulte [Crear una política de puntos de conexión](#) en la Guía EC2 del usuario de Amazon.

[EC2.12] Amazon no utilizado EC2 EIPs debería retirarse

Requisitos relacionados: PCI DSS v3.2.1/2.4, NIST.800-53.r5 CM-8 (1)

Categoría: Proteger - Configuración de red segura

Gravedad: baja

Tipo de recurso: AWS :: EC2 :: EIP

Regla de AWS Config : [eip-attached](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las direcciones IP elásticas (EIP) que están asignadas a una VPC están asociadas a instancias o EC2 a interfaces de red elásticas en uso (). ENIs

Un error en el resultado indica que puede no utilizarse EC2 EIPs.

Esto le ayudará a mantener un inventario de activos preciso EIPs en su entorno de datos de titulares (CDE).

Corrección

Para obtener una EIP que no está en uso, consulte [Lanzamiento de una dirección IP elástica](#) en la Guía del EC2 usuario de Amazon.

[EC2.13] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0.0.0/0 o :/0 al puerto 22

Requisitos relacionados: NIST.800-171.2.0/4.1, (21), (11), (11) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (21), (4) NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 SC-7 NIST.800-171.1.r1.1.1.1.1.1.2 3.2.1/1.2.1,

NIST.800-53.r5 SC-7 PCI AWS DSS v3.2.1/1.2.1/1.3.1, PCI DSS v3.2.1/2.1/2.0/1.3.1, PCI DSS v3.2.1/2.1/2.0/1.3.1 SS v4.0.1/1.3.1 NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: AWS::EC2::SecurityGroup

Regla de AWS Config : [restricted-ssh](#)

Tipo de programa: activado por cambios y periódico

Parámetros: ninguno

Este control comprueba si un grupo de EC2 seguridad de Amazon permite la entrada desde 0.0.0.0/0 o :/0 al puerto 22. Se produce un error en el control si el grupo de seguridad permite la entrada desde 0.0.0.0/0 o :/0 al puerto 22.

Los grupos de seguridad proporcionan filtrado con estado del tráfico de red de entrada y salida a los recursos de AWS . Recomendamos que ningún grupo de seguridad permita el acceso de entrada ilimitado al puerto 22. La eliminación de la conectividad libre a los servicios de la consola a distancia, como SSH, reduce la exposición al riesgo del servidor.

Corrección

Para prohibir la entrada al puerto 22, elimine la regla que permite dicho acceso a cada grupo de seguridad asociado a una VPC. Para obtener instrucciones, consulta [Actualizar las reglas de los grupos de seguridad](#) en la Guía del EC2 usuario de Amazon. Después de seleccionar un grupo de seguridad en la EC2 consola de Amazon, elija Acciones y editar reglas de entrada. Elimine la regla que permite el acceso al puerto 22.

[EC2.14] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0.0.0/0 o :/0 al puerto 3389

Requisitos relacionados: Indicador de referencia de CIS AWS v1.2.0/4.2, PCI DSS v4.0.1/1.3.1

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: AWS::EC2::SecurityGroup

AWS Config regla [restricted-common-ports](#): (restricted-rdpla regla creada es)

Tipo de programa: activado por cambios y periódico

Parámetros: ninguno

Este control comprueba si un grupo de EC2 seguridad de Amazon permite la entrada desde 0.0.0.0 o ::/0 al puerto 3389. Se produce un error en el control si el grupo de seguridad permite la entrada desde 0.0.0.0/0 o ::/0 al puerto 3389.

Los grupos de seguridad proporcionan filtrado con estado del tráfico de red de entrada y salida a los recursos de AWS . Recomendamos que ningún grupo de seguridad permita el acceso de entrada ilimitado al puerto 3389. La eliminación de la conectividad libre a los servicios de la consola a distancia, como RDP, reduce la exposición al riesgo del servidor.

Corrección

Para prohibir la entrada al puerto 3389, elimine la regla que permite dicho acceso a cada grupo de seguridad asociado a una VPC. Para obtener instrucciones, consulte [Actualizar reglas del grupo de seguridad](#) en la Guía del usuario de Amazon VPC. Tras seleccionar un grupo de seguridad en la consola de Amazon VPC, elija Acciones y editar reglas de entrada. Elimine la regla que permite el acceso al puerto 3389.

[EC215] EC2 Las subredes de Amazon no deben asignar automáticamente direcciones IP públicas

Requisitos relacionados: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.4.4

Categoría: Proteger > Seguridad de red

Gravedad: media

Tipo de recurso: AWS::EC2::Subnet

Regla de AWS Config : [subnet-auto-assign-public-ip-disabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la asignación de subredes públicas IPs en la Amazon Virtual Private Cloud (Amazon VPC) se ha MapPublicIpOnLaunch establecido en. FALSE El control pasa si el indicador está establecido como FALSE.

Todas las subredes tienen un atributo que determina si una interfaz de red creada en la subred recibe automáticamente una dirección pública IPv4 . Las instancias que se lanzan a subredes que tienen este atributo habilitado tienen una dirección IP pública asignada a su interfaz de red principal.

Corrección

Si desea configurar una subred para que no asigne direcciones IP públicas, consulte [Modificación del atributo de IPv4 direcciones públicas de su subred](#) en la Guía del usuario de Amazon VPC. Desactive la casilla Habilitar la asignación automática de IPv4 direcciones públicas.

[EC2.16] Deben eliminarse las listas de control de acceso a la red no utilizadas

Requisitos relacionados: NIST.800-53.r5 CM-8 (1), NIST.800-171.r2 3.4.7, PCI DSS v4.0.1/1.2.7

Categoría: Proteger > Seguridad de red

Gravedad: baja

Tipo de recurso: AWS::EC2::NetworkACL

Regla de AWS Config : [vpc-network-acl-unused-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si hay alguna lista de control de acceso de la red (red ACLs) sin utilizar en su nube privada virtual (VPC). El control lanza error si la ACL de la red no está asociada a una subred. El control no genera resultados para una ACL de red predeterminada que no está en uso.

El control comprueba la configuración de elementos del recurso de AWS::EC2::NetworkACL y determina las relaciones de la ACL de la red.

Si la única relación es la VPC de la ACL de la red, el control lanza error.

Si se enumeran otras relaciones, el control pasa.

Corrección

Para obtener instrucciones sobre cómo eliminar una ACL de red no utilizada, consulte [Eliminar una ACL de red](#) en la Guía del usuario de Amazon VPC. No puede eliminar la ACL de red predeterminada ni una ACL asociada a subredes.

[EC2.17] EC2 Las instancias de Amazon no deberían usar múltiples ENIs

Requisitos relacionados: NIST.800-53.r5 AC-4 (21)

Categoría: Proteger > Seguridad de red

Gravedad: baja

Tipo de recurso: AWS::EC2::Instance

Regla de AWS Config : [ec2-instance-multiple-eni-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una EC2 instancia utiliza varias interfaces de red elásticas (ENIs) o adaptadores de estructura elástica (EFAs). Este control se ejecuta si se utiliza un único adaptador de red. El control incluye una lista de parámetros opcional para identificar los permitidos ENIs. Este control también falla si una EC2 instancia que pertenece a un clúster de Amazon EKS utiliza más de un ENI. Si sus EC2 instancias necesitan tener varias instancias ENIs como parte de un clúster de Amazon EKS, puede ocultar esos resultados de control.

Si hay varias ENIs instancias de doble host, es decir, instancias que tienen varias subredes. Esto puede añadir complejidad a la seguridad de la red e introducir rutas y accesos a la red no deseados.

Corrección

Para desvincular una interfaz de red de una EC2 instancia, consulte [Desvinculación de una interfaz de red de una instancia](#) en la Guía del EC2 usuario de Amazon.

[EC2.18] Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados

Requisitos relacionados: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4, (11), (16) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 SC-7 NIST.800-171.r2 NIST.800-53.r5 SC-7 3.1.3, NIST.800-171.r2 3.1.20, NIST.800-171.r2 3.13.1

Categoría: Proteger > Configuración de red segura > Configuración de grupos de seguridad

Gravedad: alta

Tipo de recurso: AWS::EC2::SecurityGroup

Regla de AWS Config : [vpc-sg-open-only-to-authorized-ports](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
authorizeTcpPorts	Lista de puertos TCP autorizados	IntegerList (1 elemento como mínimo y 32 elementos como máximo)	De 1 a 65535	[80, 443]
authorizeUdpPorts	Lista de puertos UDP autorizados	IntegerList (1 elemento como mínimo y 32 elementos como máximo)	De 1 a 65535	Sin valor predeterminado

Este control comprueba si un grupo de EC2 seguridad de Amazon permite el tráfico entrante sin restricciones de puertos no autorizados. El estado de control se determina de la siguiente manera:

- Si se utiliza el valor predeterminado para `authorizedTcpPorts`, se producirá un error en el control si el grupo de seguridad permite el tráfico entrante sin restricciones de cualquier puerto que no sea el 80 ni el 443.
- Si proporciona valores personalizados para `authorizedTcpPorts` o `authorizedUdpPorts`, se producirá un error en el control si el grupo de seguridad permite el tráfico entrante sin restricciones de cualquier puerto que no figure en la lista.

Los grupos de seguridad proporcionan filtrado con estado del tráfico de red de entrada y salida a AWS. Las reglas de los grupos de seguridad deben seguir el principio del acceso con menos privilegios. El acceso sin restricciones (dirección IP con sufijo /0) aumenta la posibilidad de actividades maliciosas, como piratería, denial-of-service ataques y pérdida de datos. A menos que se permita específicamente un puerto, dicho puerto debería denegar el acceso sin restricciones.

Corrección

Para modificar un grupo de seguridad, consulte [Trabajo con grupos de seguridad](#) en la Guía del usuario de Amazon VPC.

[EC219] Los grupos de seguridad no deben permitir el acceso irrestricto a los puertos de alto riesgo

Requisitos relacionados: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4, (1), NIST.800-53.r5 CA-9 (11), (16) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 SC-7 NIST.800-171.r2 NIST.800-53.r5 SC-7 3.1.3, NIST.800-171.r2 3.1.20, NIST.800-171.r2 3.13.1

Categoría: Proteger > Acceso restringido a la red

Gravedad: crítica

Tipo de recurso: AWS::EC2::SecurityGroup

AWS Config regla [restricted-common-ports](#) vpc-sg-restricted-common-ports: (la regla creada es)

Tipo de programa: activado por cambios y periódico

Parámetros: "blockedPorts":

"20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,5600"
(no personalizables)

Este control comprueba si el tráfico ilimitado entrante de un grupo de EC2 seguridad de Amazon es accesible para los puertos especificados que se consideran de mayor riesgo. Este control falla si alguna de las reglas de un grupo de seguridad permite la entrada de tráfico desde "0.0.0.0/0" o "::/0" a esos puertos.

Los grupos de seguridad proporcionan filtrado con estado del tráfico de red de entrada y salida a los recursos de AWS . El acceso ilimitado (0.0.0.0) aumenta las oportunidades de actividades maliciosas, como piratería, denial-of-service ataques y pérdida de datos. Ningún grupo de seguridad debe permitir el acceso de entrada sin restricciones a los siguientes puertos:

- 20, 21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)
- POP3(10)
- 135 (RPC)
- 143 (IMAP)
- 445 (CIFS)
- 1433, 1434 (MSSQL)
- 3000 (marcos de desarrollo web Go, Node.js y Ruby)
- 3306 (MySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000 (marcos de desarrollo web Python)
- 5432 (postgresql)
- 500 (fcp-addr-srvr1)
- 5601 (OpenSearch Dashboards)
- 8080 (proxy)
- 8088 (puerto HTTP antiguo)
- 8888 (puerto HTTP alternativo)

- 9200 o 9300 () OpenSearch

Corrección

Para eliminar reglas de un grupo de seguridad, consulte [Eliminar reglas de un grupo de seguridad](#) en la Guía del EC2 usuario de Amazon.

[EC220] Ambos túneles de VPN de una conexión de AWS Site-to-Site VPN deben estar activos

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), NIST.800-53.r5 SI-13 SI-13 SI-13 SI-13 SI-13 SI-13 (5), NIST.800-53.r5 SI-13 (5), NIST.800-53.r5 SI-13 SI-13 SI-13 SI-13 SI-13 SI-13 SI-13 SI-13 SI-13 SI-13

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso:AWS::EC2::VPNConnection

Regla de AWS Config : [vpc-vpn-2-tunnels-up](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Un túnel VPN es un enlace cifrado donde los datos pueden pasar entre la red del cliente AWS y una conexión AWS Site-to-Site VPN. Cada conexión de VPN incluye dos túneles de VPN que puede utilizar simultáneamente para conseguir alta disponibilidad. Asegurarse de que ambos túneles VPN estén activos para una conexión VPN es importante para confirmar una conexión segura y de alta disponibilidad entre una AWS VPC y su red remota.

Este control comprueba que los dos túneles VPN proporcionados por AWS Site-to-Site VPN estén en estado activo. El control falla si uno o ambos túneles están en estado INACTIVO.

Corrección

Para modificar las opciones del túnel de la VPN, consulte [Modificación Site-to-Site de las opciones del túnel](#) de la AWS Site-to-Site VPN en la Guía del usuario de la VPN.

[EC2.21] La red no ACLs debe permitir la entrada desde 0.0.0/0 al puerto 22 o al puerto 3389

Requisitos relacionados: AWS NIST.800-171.4.0/5.1, NIST.800-171.0/5.1, AWS NIST.800-171.21, (21), (21), NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 CA-9, NIST.800-171.1.r2 NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 3.1.800-171.r2 3.1.1.800-171.r2 3.13.1, PCI DSS v4.0.1/1.3.1

Categoría: Proteger > Configuración de red segura

Gravedad: media

Tipo de recurso: AWS::EC2::NetworkAcl

Regla de AWS Config : [nacl-no-unrestricted-ssh-rdp](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una lista de control de acceso de la red (ACL de la red) permite el acceso sin restricciones a los puertos TCP predeterminados para el tráfico de entrada SSH/RDP. El control lanza error si una entrada entrante de la ACL de la red permite un bloque de CIDR de origen de "0.0.0.0/0" o ":::/0" para los puertos TCP 22 o 3389. El control no genera resultados para una ACL de red predeterminada.

El acceso a los puertos de administración remota del servidor, como el puerto 22 (SSH) y el puerto 3389 (RDP), no debe ser de acceso público, ya que esto puede permitir el acceso no deseado a los recursos de la VPC.

Corrección

Para editar las reglas de tráfico de ACL de la red, consulte [Trabajar con la red ACLs](#) en la Guía del usuario de Amazon VPC.

[EC2.22] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse

Categoría: Identificar - Inventario

Gravedad: media

Tipo de recurso: AWS::EC2::NetworkInterface, AWS::EC2::SecurityGroup

Regla de AWS Config : [ec2-security-group-attached-to-eni-periodic](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si los grupos de seguridad están asociados a instancias de Amazon Elastic Compute Cloud (Amazon EC2) o a una interfaz de red elástica. El control falla si el grupo de seguridad no está asociado a una EC2 instancia de Amazon o a una elastic network.

 Important

El 20 de septiembre de 2023, Security Hub eliminó este control de las AWS Foundational Security Best Practices y del NIST SP 800-53, revisión 5. Este control sigue formando parte del estándar de administración de servicios. AWS Control Tower Este control produce un resultado aprobado si los grupos de seguridad están conectados a EC2 instancias o a una interface de red elástica. Sin embargo, en algunos casos de uso, los grupos de seguridad independientes no representan un riesgo para la seguridad. Puede usar otros EC2 controles, como EC2 .2, EC2 .13, EC2 .14, EC2 .18 y EC2 .19, para monitorear sus grupos de seguridad.

Corrección

Para crear, asignar y eliminar grupos de seguridad, consulta [Grupos de seguridad para tus EC2 instancias](#) en la Guía del EC2 usuario de Amazon.

[EC2.23] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC

Requisitos relacionados: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: AWS::EC2::TransitGateway

Regla de AWS Config : [ec2-transit-gateway-auto-vpc-attach-disabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las pasarelas de EC2 tránsito aceptan automáticamente adjuntos de VPC compartidos. Este control falla en el caso de una pasarela de tránsito que acepta automáticamente las solicitudes de adjuntos de VPC compartidas.

Al activar `AutoAcceptSharedAttachments` se configura una pasarela de tránsito para que acepte automáticamente cualquier solicitud de adjunto de VPC multicuenta sin verificar la solicitud o la cuenta desde la que se origina el archivo adjunto. Para seguir las prácticas recomendadas de autorización y autenticación, recomendamos desactivar esta característica para garantizar que solo se acepten las solicitudes de adjuntos de VPC autorizadas.

Corrección

Para modificar una puerta de enlace de tránsito, consulte [Modificación de una puerta de enlace de tránsito](#) en la Guía para desarrolladores de Amazon VPC.

[EC224] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: media

Tipo de recurso: AWS::EC2::Instance

Regla de AWS Config : [ec2-paravirtual-instance-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el tipo de virtualización de una EC2 instancia es paravirtual. El control falla si `virtualizationType` la EC2 instancia está configurada en `paravirtual`.

Las Imágenes de máquina de Amazon (AMIs) de Linux utilizan uno de los dos tipos de virtualización: paravirtual (PV) o máquina virtual de hardware (HVM). Las principales diferencias entre PV y HVM AMIs son la forma en que arrancan y si son o no compatibles con extensiones de hardware especiales (CPU, red y almacenamiento) para lograr un mejor desempeño.

Antes, el rendimiento de los invitados PV era mejor que el de los invitados HVM en muchos casos, pero esto ya no es así debido a las mejoras de la virtualización HVM y a la disponibilidad de controladores PV para HVM AMIs. Para obtener más información, consulte [Tipos de virtualización de AMI de Linux](#) en la Guía del EC2 usuario de Amazon.

Corrección

Para actualizar una EC2 instancia a un nuevo tipo de instancia, consulta [Cambiar el tipo de instancia](#) en la Guía del EC2 usuario de Amazon.

[EC2.25] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red

Requisitos relacionados: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.4.4

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso:AWS::EC2::LaunchTemplate

Regla de AWS Config : [ec2-launch-template-public-ip-disabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las plantillas de EC2 lanzamiento de Amazon están configuradas para asignar direcciones IP públicas a las interfaces de red en el momento del lanzamiento. El control falla si una plantilla de EC2 lanzamiento está configurada para asignar una dirección IP pública a las interfaces de red o si hay al menos una interfaz de red que tiene una dirección IP pública.

Una dirección IP pública es una dirección a la que se puede tener acceso desde Internet. Si configura las interfaces de red con una dirección IP pública, es posible que se pueda acceder a los recursos asociados a esas interfaces de red desde Internet. EC2 los recursos no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a sus cargas de trabajo.

Corrección

Para actualizar una plantilla de EC2 lanzamiento, consulte [Cambiar la configuración de la interfaz de red predeterminada](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

[EC2.28] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Gravedad: baja

Tipo de recurso: AWS::EC2::Volume

AWS Config regla: [ebs-resources-protected-by-backup-plan](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
backupVaultLockCheck	El control produce un PASSED resultado si el parámetro está establecido en true y el recurso utiliza el Bloqueo de AWS Backup almacenes de.	Booleano	true o false	Sin valor predeterminado

Este control evalúa si un volumen de Amazon EBS en el estado in-use está cubierto por un plan de copias de seguridad. Se produce un error en el control si un volumen de Amazon EBS no está cubierto por un plan de copias de seguridad. Si establece el backupVaultLockCheck parámetro en

un valor igual a true, el control solo pasa si el volumen de EBS está guardada en un almacén AWS Backup bloqueado de.

Las copias de seguridad le ayudan a recuperarse más rápidamente de un incidente de seguridad. También refuerzan la resiliencia de sus sistemas. La inclusión de los volúmenes de Amazon EBS en un plan de copias de seguridad le ayuda a proteger sus datos contra pérdidas o eliminaciones involuntarias.

Corrección

Para añadir un volumen de Amazon EBS a un plan de AWS Backup copias de seguridad de, consulte [Asignación de recursos a un plan de copias](#) de seguridad en la Guía para AWS Backup desarrolladores.

[EC2.33] Las conexiones de puerta de enlace de EC2 tránsito deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::TransitGatewayAttachment

Regla de AWS Config : tagged-ec2-transitgatewayattachment (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si el archivo adjunto de una puerta de enlace de EC2 tránsito de Amazon tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la conexión de puerta de enlace de tránsito no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la conexión de puerta de enlace de tránsito no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un archivo adjunto de EC2 Transit Gateway, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.34] Las tablas de enrutamiento de las puertas de enlace de EC2 tránsito deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::TransitGatewayRouteTable`

Regla de AWS Config : `tagged-ec2-transitgatewayroutetable` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una tabla de enrutamiento de Amazon EC2 Transit Gateway tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la tabla de enrutamiento de la puerta de enlace de tránsito no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la tabla de enrutamiento de la puerta de enlace de tránsito no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de.

Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una tabla de rutas de una pasarela de EC2 transporte, consulta [Cómo etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.35] Las interfaces EC2 de red deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::NetworkInterface

Regla de AWS Config : tagged-ec2-networkinterface (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.		que cumplan con AWS los requisitos .	

Este control comprueba si una interfaz de EC2 red de Amazon tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la interfaz de red no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la interfaz de red no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una interfaz de EC2 red, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.36] Las pasarelas de EC2 clientes deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::CustomerGateway

Regla de AWS Config : tagged-ec2-customergateway (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una puerta de enlace de EC2 cliente de Amazon tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la puerta de enlace de cliente no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la puerta de enlace de cliente no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una pasarela de EC2 clientes, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.37] Las direcciones IP EC2 elásticas deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS : : EC2 : : EIP

Regla de AWS Config : tagged-ec2-eip (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una dirección IP EC2 elástica de Amazon Elastic tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la dirección IP elástica no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la dirección IP elástica no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing.

Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una dirección IP EC2 elástica, consulta [Etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.38] EC2 las instancias deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::Instance

Regla de AWS Config : tagged-ec2-instance (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una EC2 instancia de Amazon tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la instancia no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una

clave de etiqueta y lanza error si la instancia no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una EC2 instancia, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.39] Las puertas de enlace de EC2 Internet deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::InternetGateway

Regla de AWS Config : tagged-ec2-internetgateway (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una puerta de enlace de EC2 Internet de Amazon tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la puerta de enlace de Internet no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la puerta de enlace de Internet no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing.

Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una pasarela de EC2 Internet, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.40] Las puertas de enlace de EC2 NAT deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::NatGateway

Regla de AWS Config : tagged-ec2-natgateway (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una puerta de enlace de traducción de direcciones de EC2 red (NAT) de Amazon tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la puerta de enlace de NAT no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y

lanza error si la puerta de enlace de NAT no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws :`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una puerta de enlace EC2 NAT, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

La EC2 red [EC2.41] ACLs debe estar etiquetada

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::NetworkACL`

Regla de AWS Config : `tagged-ec2-networkacl` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una lista de control de acceso (ACL de la red) de Amazon EC2 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la ACL de la red no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la ACL de la red no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws :`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing.

Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una ACL EC2 de red, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.42] Las tablas de EC2 enrutamiento deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::RouteTable

Regla de AWS Config : tagged-ec2-routetable (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una tabla de EC2 enrutamiento de Amazon tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la tabla de enrutamiento no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la tabla de enrutamiento no

está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una tabla de EC2 rutas, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.43] los grupos EC2 de seguridad deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::SecurityGroup`

Regla de AWS Config : `tagged-ec2-securitygroup` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si el grupo EC2 de seguridad de Amazon tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el grupo de seguridad no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el grupo de seguridad no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing.

Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un grupo EC2 de seguridad, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

EC2 Las subredes [EC2.44] deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::Subnet

Regla de AWS Config : tagged-ec2-subnet (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una EC2 subred de Amazon tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la subred no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si

no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la subred no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una EC2 subred, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.45] los EC2 volúmenes deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::Volume

Regla de AWS Config : tagged-ec2-volume (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si el EC2 volumen de Amazon tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el volumen no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el volumen no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing.

Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un EC2 volumen, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.46] Amazon VPCs debería estar etiquetado

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::VPC

Regla de AWS Config : tagged-ec2-vpc (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una Amazon Virtual Private Cloud (Amazon VPC) tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la Amazon VPC no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el

control solo comprueba la existencia de una clave de etiqueta y lanza error si la Amazon VPC no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una VPC, consulte [Etiquetar los EC2 recursos de Amazon](#) en la Guía EC2 del usuario de Amazon.

[EC2.47] Los servicios de puntos de conexión de Amazon VPC deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::VPCEndpointService`

Regla de AWS Config : `tagged-ec2-vpcendpointservice` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un servicio de puntos de conexión de Amazon VPC tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el servicio de punto de conexión no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el servicio de punto de conexión no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws :`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un servicio de punto de conexión de Amazon VPC, consulte [Administración de etiquetas](#) en la sección [Configuración de un servicio de punto de conexión](#) de la Guía AWS PrivateLink .

[EC2.48] Los registros de flujo de Amazon VPC deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::FlowLog

Regla de AWS Config : tagged-ec2-flowlog (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un registro de flujo de Amazon VPC tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el registro de flujo no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el registro de flujo no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un registro de flujo de Amazon VPC, consulte [Etiquetado de un registro de flujo](#) en la Guía del usuario de Amazon VPC.

[EC2.49] Las conexiones de emparejamiento de Amazon VPC deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::VPCPeeringConnection`

Regla de AWS Config : `tagged-ec2-vpcpeeringconnection` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una conexión de emparejamiento de Amazon VPC tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la conexión de emparejamiento no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la conexión de emparejamiento no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades

principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una conexión de emparejamiento de Amazon VPC, consulta [Cómo etiquetar tus EC2 recursos de Amazon](#) en la Guía del usuario de Amazon EC2 .

[EC2.50] Las puertas de enlace de EC2 VPN deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::VPNGateway

Regla de AWS Config : tagged-ec2-vpngateway (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.		que cumplan con AWS los requisitos .	

Este control comprueba si una puerta de enlace de Amazon EC2 VPN tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la puerta de enlace VPN no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la puerta de enlace VPN no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una puerta de enlace EC2 VPN, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC251] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), (4), (26), NIST.800-53.r5 AC-2 (9), NIST.800-53.r5 AC-4 NIST.800-53.r5 SI-3 NIST.800-53.r5 AC-6 (8), NIST.800-53.r5 SI-4 NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-4 NIST.800-53.r5 SC-7 (20), NIST.800-171.r2 3.1.1.1.1.R2 3.1.1.1.12, NIST.800-171.r2 3.1.1.1.12, NIST.800-171.r2 3.1.1.20, PCI DSS v4.0.1/10.2.1

Categoría: Identificar - Registro

Gravedad: baja

Tipo de recurso: AWS::EC2::ClientVpnEndpoint

AWS Config regla: [ec2-client-vpn-connection-log-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un AWS Client VPN punto de conexión de tiene activado el registro de conexiones de clientes. Se produce un error en el control si el punto de conexión no tiene habilitado el registro de conexiones de clientes.

Los puntos de conexión de Client VPN permiten a los clientes remotos conectarse de manera segura a los recursos de una nube privada virtual (VPC) en AWS. Los registros de conexión permiten hacer un seguimiento de la actividad de los usuarios en el punto de conexión de la VPN y proporcionan visibilidad. Cuando habilita el registro de conexión, puede especificar el nombre de una secuencia de registros en el grupo de registros. Si no se especifica ningún flujo de registros, el servicio Client VPN crea uno automáticamente.

Corrección

Para habilitar el registro de conexión, consulte [Habilitación del registro de conexión en un punto de conexión de Client VPN existente](#) en la Guía del administrador de AWS Client VPN .

[EC2.52] Las EC2 puertas de enlace de

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::TransitGateway

Regla de AWS Config : tagged-ec2-transitgateway (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si una puerta de enlace de EC2 tránsito de Amazon tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la puerta de enlace de tránsito no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la puerta de enlace de tránsito no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios

responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una pasarela de EC2 transporte, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.53] Los grupos EC2 de seguridad no deberían permitir la entrada de 0.0.0.0/0 a los puertos de administración de servidores remotos

Requisitos relacionados: Indicador de referencia de CIS AWS v3.0.0/5.2, PCI DSS v4.0.1/1.3.1

Categoría: Proteger > Configuración de red segura > Configuración de grupos de seguridad

Gravedad: alta

Tipo de recurso: AWS::EC2::SecurityGroup

Regla de AWS Config : [vpc-sg-port-restriction-check](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
ipType	La versión de IP	Cadena	No personalizable	IPv4
restrictPorts	Lista de puertos que deben rechazar el tráfico de entrada	IntegerList	No personalizable	22, 3389

Este control comprueba si un grupo de EC2 seguridad de Amazon permite la entrada de 0.0.0.0/0 a los puertos de administración de servidores remotos (puertos 22 y 3389). El control lanza error si el grupo de seguridad permite la entrada de 0.0.0.0/0 a los puertos 22 o 3389.

Los grupos de seguridad proporcionan filtrado con estado del tráfico de red de entrada y salida a los recursos. AWS recomienda que ningún grupo de seguridad permita el acceso sin restricciones a los puertos de administración de servidores remotos, como SSH al puerto 22 y RDP al puerto 3389, mediante los protocolos TDP (6), UDP (17) o ALL (-1). Si se permite el acceso público a estos puertos, crece la superficie expuesta a ataques de los recursos y el riesgo de que los recursos se vean comprometidos.

Corrección

Para actualizar una regla de un grupo de EC2 seguridad para prohibir el tráfico de entrada a los puertos especificados, consulte [Actualización de las reglas de un grupo de seguridad](#) en la Guía del EC2 usuario de Amazon. Después de seleccionar un grupo de seguridad en la EC2 consola de Amazon, elija Acciones y editar reglas de entrada. Elimine la regla que permite el acceso a los puertos 22 o 3389.

[EC2.54] Los grupos EC2 de seguridad no deberían permitir la entrada de: :/0 a los puertos de administración de servidores remotos

Requisitos relacionados: Indicador de referencia de CIS AWS v3.0.0/5.3, PCI DSS v4.0.1/1.3.1

Categoría: Proteger > Configuración de red segura > Configuración de grupos de seguridad

Gravedad: alta

Tipo de recurso: AWS::EC2::SecurityGroup

Regla de AWS Config : [vpc-sg-port-restriction-check](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
ipType	La versión de IP	Cadena	No personalizable	IPv6
restrictPorts	Lista de puertos que deben rechazar el tráfico de entrada	IntegerList	No personalizable	22, 3389

Este control comprueba si un grupo de EC2 seguridad de Amazon permite la entrada de ::/0 a los puertos de administración de servidores remotos (puertos 22 y 3389). El control lanza error si el grupo de seguridad permite la entrada de ::/0 o a los puertos 22 o 3389.

Los grupos de seguridad proporcionan filtrado con estado del tráfico de red de entrada y salida a los recursos. AWS recomienda que ningún grupo de seguridad permita el acceso sin restricciones a los puertos de administración de servidores remotos, como SSH al puerto 22 y RDP al puerto 3389, mediante los protocolos TDP (6), UDP (17) o ALL (-1). Si se permite el acceso público a estos puertos, crece la superficie expuesta a ataques de los recursos y el riesgo de que los recursos se vean comprometidos.

Corrección

Para actualizar una regla de un grupo de EC2 seguridad para prohibir el tráfico de entrada a los puertos especificados, consulte [Actualización de las reglas de un grupo de seguridad](#) en la Guía del EC2 usuario de Amazon. Tras seleccionar un grupo de seguridad en la EC2 consola de Amazon, elija Acciones y editar reglas de entrada. Elimine la regla que permite el acceso a los puertos 22 o 3389.

[EC2.55] VPCs debe configurarse con un punto final de interfaz para la API ECR

Requisitos relacionados: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (4)

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Gravedad: media

Tipo de recurso: AWS::EC2::VPC, AWS::EC2::VPCEndpoint

Regla de AWS Config : [vpc-endpoint-enabled](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Obligatorio	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
serviceNames	Obligatorio	El nombre del servicio que evalúa el control	Cadena	No personalizable	ecr.api
vpcIds	Opcional	Lista separada por comas de Amazon VPC IDs para puntos de conexión de VPC.	StringList	Personalice con una o más VPC IDs	Sin valor predeterminado

Parámetro	Obligatorio	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
		Si se proporciona, el control falla si los servicios especificados en el serviceName parámetro no tienen uno de estos puntos de conexión de VPC.			

Este control comprueba si una nube privada virtual (VPC) gestionada tiene un punto de enlace de VPC de interfaz para la API de Amazon ECR. Se produce un error en el control si la VPC no tiene un punto de conexión de VPC de interfaz para la API de ECR. Este control evalúa los recursos en una sola cuenta.

AWS PrivateLink permite a los clientes acceder a los servicios alojados AWS en ellos de una manera escalable y de alta disponibilidad, manteniendo todo el tráfico de la red dentro de la AWS red. Los usuarios del servicio pueden acceder de forma privada a los servicios con tecnología PrivateLink desde su VPC o sus instalaciones locales, sin utilizar el público IPs y sin necesidad de que el tráfico atraviese Internet.

Corrección

Para configurar un punto de enlace de VPC, consulte [Acceder y Servicio de AWS utilizar un punto de enlace de VPC](#) de interfaz en la Guía.AWS PrivateLink

[EC2.56] VPCs debe configurarse con un punto final de interfaz para Docker Registry

Requisitos relacionados: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (4)

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Gravedad: media

Tipo de recurso: AWS::EC2::VPC, AWS::EC2::VPCEndpoint

Regla de AWS Config : [vpc-endpoint-enabled](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Obligatorio	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
serviceNames	Obligatorio	El nombre del servicio que evalúa el control	Cadena	No personalizable	ecr.dkr
vpcIds	Opcional	Lista separada por comas de Amazon VPC IDs para	StringList	Personalice con uno o más VPC IDs	Sin valor predeterminado

Parámetro	Obligatorio	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
		puntos de conexión de VPC. Si se proporciona, el control falla si los servicios especificados en el serviceName parámetro no tienen uno de estos puntos de conexión de VPC.			

Este control comprueba si una nube privada virtual (VPC) administrada tiene un punto de enlace de VPC de interfaz para Docker Registry. Se produce un error en el control si la VPC no tiene un punto de conexión de VPC de interfaz para Docker Registry. Este control evalúa los recursos en una sola cuenta.

AWS PrivateLink permite a los clientes acceder a los servicios alojados AWS en ellos de una manera escalable y de alta disponibilidad, manteniendo todo el tráfico de la red dentro de la AWS red. Los usuarios del servicio pueden acceder de forma privada a los servicios con tecnología PrivateLink desde su VPC o sus instalaciones locales, sin utilizar el público IPs y sin necesidad de que el tráfico atraviese Internet.

Corrección

Para configurar un punto de enlace de VPC, consulte [Acceder y Servicio de AWS utilizar un punto de enlace de VPC](#) de interfaz en la Guía.AWS PrivateLink

[EC2.57] VPCs debe configurarse con un punto final de interfaz para Systems Manager

Requisitos relacionados: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Gravedad: media

Tipo de recurso: AWS::EC2::VPC, AWS::EC2::VPCEndpoint

Regla de AWS Config : [vpc-endpoint-enabled](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Obligatorio	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
serviceNames	Obligatorio	El nombre del servicio que evalúa el control	Cadena	No personalizable	ssm
vpcIds	Opcional	Lista separada por comas	StringList	Personalice con una	Sin valor predeterminado

Parámetro	Obligatorio	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
		de Amazon VPC IDs para puntos de conexión de VPC. Si se proporciona, el control falla si los servicios especificados en el serviceName parámetro no tienen uno de estos puntos de conexión de VPC.		o más VPC IDs	

Este control comprueba si una nube privada virtual (VPC) administrada tiene un punto de conexión de VPC de interfaz para. AWS Systems Manager Se produce un error en el control si la VPC no tiene un punto de conexión de VPC de interfaz para Systems Manager. Este control evalúa los recursos en una sola cuenta.

AWS PrivateLink permite a los clientes acceder a los servicios alojados AWS en ellos de una manera escalable y de alta disponibilidad, manteniendo todo el tráfico de la red dentro de la AWS red. Los

usuarios del servicio pueden acceder de forma privada a los servicios con tecnología PrivateLink desde su VPC o sus instalaciones locales, sin utilizar el público IPs y sin necesidad de que el tráfico atraviese Internet.

Corrección

Para configurar un punto de enlace de VPC, consulte [Acceder y Servicio de AWS utilizar un punto de enlace de VPC](#) de interfaz en la Guía.AWS PrivateLink

[EC2.58] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager

Requisitos relacionados: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Gravedad: media

Tipo de recurso: AWS::EC2::VPC, AWS::EC2::VPCEndpoint

Regla de AWS Config : [vpc-endpoint-enabled](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Obligatorio	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
serviceNames	Obligatorio	El nombre del servicio que evalúa el control	Cadena	No personalizable	ssm-contacts

Parámetro	Obligatorio	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
vpcIds	Opcional	Lista separada por comas de Amazon VPC IDs para puntos de conexión de VPC. Si se proporciona, el control falla si los servicios especificados en el serviceName parámetro no tienen uno de estos puntos de conexión de VPC.	StringList	Personalice con una o más VPC IDs	Sin valor predeterminado

Este control comprueba si una nube privada virtual (VPC) administrada tiene un punto de enlace de VPC de interfaz para AWS Systems Manager contactos de Incident Manager. El control falla si

la VPC no tiene un punto final de VPC de interfaz para los contactos de Systems Manager Incident Manager. Este control evalúa los recursos en una sola cuenta.

AWS PrivateLink permite a los clientes acceder a los servicios alojados AWS en ellos de una manera escalable y de alta disponibilidad, manteniendo todo el tráfico de la red dentro de la AWS red. Los usuarios del servicio pueden acceder de forma privada a los servicios con tecnología PrivateLink desde su VPC o sus instalaciones locales, sin utilizar el público IPs y sin necesidad de que el tráfico atravesase Internet.

Corrección

Para configurar un punto de enlace de VPC, consulte [Acceder y Servicio de AWS utilizar un punto de enlace de VPC](#) de interfaz en la Guía.AWS PrivateLink

[EC2.60] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager

Requisitos relacionados: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Gravedad: media

Tipo de recurso: AWS::EC2::VPC, AWS::EC2::VPCEndpoint

Regla de AWS Config : [vpc-endpoint-enabled](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Obligatorio	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>serviceName</code>	Obligatorio	El nombre del servicio que evalúa el control	Cadena	No personalizable	<code>ssm-incidents</code>
<code>vpcIds</code>	Opcional	Lista separada por comas de Amazon VPC IDs para puntos de conexión de VPC. Si se proporciona, el control falla si los servicios especificados en el <code>serviceName</code> parámetro no tienen uno de estos puntos de	StringList	Personalice con una o más VPC IDs	Sin valor predeterminado

Parámetro	Obligatorio	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
		conexión de VPC.			

Este control comprueba si una nube privada virtual (VPC) administrada tiene un punto de enlace de VPC de interfaz para Incident Manager. AWS Systems Manager El control falla si la VPC no tiene un punto final de VPC de interfaz para Systems Manager Incident Manager. Este control evalúa los recursos en una sola cuenta.

AWS PrivateLink permite a los clientes acceder a los servicios alojados AWS en ellos de una manera escalable y de alta disponibilidad, manteniendo todo el tráfico de la red dentro de la AWS red. Los usuarios del servicio pueden acceder de forma privada a los servicios con tecnología PrivateLink desde su VPC o sus instalaciones locales, sin utilizar el público IPs y sin necesidad de que el tráfico atraviese Internet.

Corrección

Para configurar un punto de enlace de VPC, consulte [Acceder y Servicio de AWS utilizar un punto de enlace de VPC](#) de interfaz en la Guía.AWS PrivateLink

[EC2.170] Las plantillas de EC2 lanzamiento deben usar el servicio de metadatos de instancias versión 2 () IMDSv2

Requisitos relacionados: PCI DSS v4.0.1/2.2.6

Categoría: Proteger > Seguridad de red

Gravedad: baja

Tipo de recurso: AWS::EC2::LaunchTemplate

Regla de AWS Config : [ec2-launch-template-imdsv2-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una plantilla de EC2 lanzamiento de Amazon está configurada con el servicio de metadatos de la instancia versión 2 (IMDSv2). El control tiene errores si `HttpTokens` está configurado como `optional`,

El uso de recursos con versiones de software compatibles garantiza un rendimiento óptimo, seguridad y acceso a las características más recientes. Las actualizaciones periódicas protegen contra las vulnerabilidades, lo que ayuda a garantizar una experiencia de usuario estable y eficaz.

Corrección

Para solicitarlo IMDSv2 en una plantilla de EC2 lanzamiento, consulte [Configurar las opciones del servicio de metadatos de instancias](#) en la Guía del EC2 usuario de Amazon.

[EC2.171] Las conexiones EC2 VPN deben tener el registro habilitado

Requisitos relacionados: Indicador de referencia de CIS AWS v3.0.0/5.3, PCI DSS v4.0.1/10.4.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::EC2::VPNConnection`

Regla de AWS Config : [ec2-vpn-connection-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una conexión de AWS Site-to-Site VPN tiene CloudWatch registros de Amazon Logs habilitados para ambos túneles. Se produce un error en el control si una conexión de Site-to-Site VPN no tiene CloudWatch registros habilitados para ambos túneles.

AWS Site-to-Site Los registros de VPN le proporcionan una mayor visibilidad de las implementaciones de Site-to-Site VPN. Con esta característica, tiene acceso a los registros de conexión de Site-to-Site VPN que proporcionan detalles sobre el establecimiento del túnel de seguridad IP (IPsec), las negociaciones de intercambio de claves de Internet (IKE) y los mensajes del protocolo de detección de pares muertos (DPD). **Site-to-Site** Los registros de la VPN se pueden publicar en CloudWatch registros. Esta característica proporciona a los clientes una única forma coherente de acceder y analizar registros detallados para todas las conexiones de la Site-to-Site VPN.

Corrección

Para habilitar el registro por túnel en una conexión EC2 VPN, consulte [los registros de AWS Site-to-Site VPN](#) en la Guía del usuario de AWS Site-to-Site VPN.

[EC2.172] La configuración del acceso público al bloqueo de EC2 VPC debería bloquear el tráfico de las puertas de enlace de Internet

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: media

Tipo de recurso: AWS::EC2::VPCLockPublicAccessOptions

Regla de AWS Config : ec2-vpc-bpa-internet-gateway-blocked (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
vpcBpaInternetGatewayBlockMode	Valor de cadena del modo de opciones de BPA de la VPC.	Enum	block-bidirectional , block-ingress	Sin valor predeterminado

Este control comprueba si los ajustes de Amazon EC2 VPC Block Public Access (BPA) están configurados para bloquear el tráfico de las puertas de enlace de Internet para todos los Amazon VPCs del. Cuenta de AWS El control falla si la configuración de BPA de la VPC no está configurada para bloquear el tráfico de las puertas de enlace de Internet. Para que el control pase, el BPA del VPC InternetGatewayBlockMode debe estar configurado en o. block-bidirectional block-ingress Si vpcBpaInternetGatewayBlockMode se proporciona el parámetro, el control solo pasa si el valor de BPA de la VPC InternetGatewayBlockMode coincide con el parámetro.

Si configura los ajustes de BPA de VPC para su cuenta en una, Región de AWS le permite bloquear los recursos VPCs y subredes de su propiedad en esa región para que no lleguen o sean accesibles desde Internet a través de puertas de enlace de Internet y puertas de enlace de Internet y puertas de enlace de Internet y puertas de enlace de Internet y puertas de enlace de Internet y puertas de enlace de Internet y puertas de enlace de Internet y puertas de enlace de Internet y puertas de enlace de Internet de solo salida. Si necesita subredes VPCs AND específicas para poder acceder o ser accesible desde Internet, puede excluirlas configurando las exclusiones de BPA de la VPC. Para obtener instrucciones sobre cómo crear y eliminar exclusiones, consulte [Crear y eliminar exclusiones](#) en la Guía del usuario de Amazon VPC.

Corrección

Para habilitar el BPA bidireccional a nivel de cuenta, consulte [Habilitar el modo bidireccional de BPA para su cuenta en](#) la Guía del usuario de Amazon VPC. Para habilitar el BPA de solo entrada, consulte Cambiar el modo BPA de la [VPC](#) a solo de entrada. Para habilitar el BPA de VPC en el nivel de la organización, consulte Habilitar el [BPA de la VPC](#) en el nivel de la organización.

[EC2.173] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::EC2::SpotFleet

Regla de AWS Config : [ec2-spot-fleet-request-ct-encryption-at-rest](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una solicitud de Amazon EC2 Spot Fleet permite el cifrado de todos los volúmenes de Amazon Elastic Block Store (Amazon EBS) asociados a instancias. EC2 El control falla si la solicitud de Spot Fleet no permite el cifrado de uno o más volúmenes de EBS especificados en la solicitud.

Para obtener un nivel de seguridad adicional, debe habilitar el cifrado de los volúmenes de Amazon EBS. A continuación, las operaciones de cifrado se producen en los servidores que alojan EC2 las instancias de Amazon, lo que ayuda a garantizar la seguridad tanto de los datos en reposo como de los datos en tránsito entre una instancia y su almacenamiento EBS adjunto. El cifrado de Amazon

EBS es una solución de cifrado sencilla para los recursos de EBS asociados a sus EC2 instancias. Con el cifrado de EBS, no está obligado a crear, mantener ni proteger su propia infraestructura de administración de claves. El cifrado de EBS utiliza AWS KMS keys cuando crea volúmenes cifrados.

Corrección

No existe una forma directa para cifrar un volumen de Amazon EBS existente y sin cifrar. Solo puede cifrar un volumen nuevo al crearlo.

Sin embargo, si ha habilitado el cifrado de forma predeterminada, Amazon EBS cifra volúmenes nuevos mediante la clave predeterminada para el cifrado de EBS. Si no habilita el cifrado de forma predeterminada, puede habilitarlo al crear un volumen individual. En ambos casos, puede anular la clave predeterminada para el cifrado de EBS y elegir una administrada por el cliente. AWS KMS key Para obtener más información acerca del cifrado de EBS, consulte Cifrado de [Amazon EBS](#) en la Guía del usuario de Amazon EBS.

Para obtener información sobre la creación de una solicitud de Amazon EC2 Spot Fleet, consulte [Create a Spot Fleet](#) en la Guía del usuario de Amazon Elastic Compute Cloud.

[EC2.174] Los conjuntos de opciones de EC2 DHCP deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::DHCPOptions

Regla de AWS Config : [ec2-dhcp-options-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Una lista de claves de etiquetas que no corresponden al sistema que deben	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	asignarse a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.		que cumplan con AWS los requisitos .	

Este control comprueba si un conjunto de opciones de EC2 DHCP de Amazon tiene las claves de etiqueta especificadas por el `requiredKeyTags` parámetro. El control lanza error si el conjunto de opciones no tiene ninguna clave de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no especifica ningún valor para el `requiredKeyTags` parámetro, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el conjunto de opciones no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws :` prefijo.

Una etiqueta es una marca que se crea y se asigna a un AWS recurso de. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. También pueden ayudarlo a realizar un seguimiento de las acciones y las notificaciones de los propietarios de recursos. También puede usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS Recursos de etiquetado y la Guía del usuario de Tag Editor](#).

Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles desde muchos Servicios de AWS. No se han diseñado para utilizarse con información privada o confidencial.

Corrección

Para obtener información sobre cómo añadir etiquetas a un conjunto de opciones de Amazon EC2 DHCP, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.175] Las plantillas de EC2 lanzamiento deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::LaunchTemplate

Regla de AWS Config : [ec2-launch-template-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Una lista de claves de etiquetas que no corresponden al sistema que deben asignarse a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una plantilla de EC2 lanzamiento de Amazon tiene las claves de etiqueta especificadas por el `requiredKeyTags` parámetro. El control lanza error si la plantilla de lanzamiento no tiene ninguna clave de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no se especifica ningún valor para el `requiredKeyTags` parámetro, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la

plantilla de lanzamiento no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws:` prefijo.

Una etiqueta es una marca que se crea y se asigna a un AWS recurso de. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. También pueden ayudarlo a realizar un seguimiento de las acciones y las notificaciones de los propietarios de recursos. También puede usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS Recursos de etiquetado y la Guía del usuario de Tag Editor](#).

 Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles desde muchos Servicios de AWS. No se han diseñado para usarse con información privada o confidencial.

Corrección

Para obtener información sobre cómo añadir etiquetas a una plantilla de EC2 lanzamiento de Amazon, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.176] Las listas de EC2 prefijos deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EC2::PrefixList`

Regla de AWS Config : [ec2-prefix-list-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Una lista de claves de etiquetas que no corresponden al sistema que deben asignarse a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una lista de EC2 prefijos de Amazon tiene las claves de etiquetas especificadas por el `requiredKeyTags` parámetro. El control lanza error si la lista de prefijos no tiene ninguna clave de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no especifica ningún valor para el `requiredKeyTags` parámetro, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la lista de prefijos no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws :` prefijo.

Una etiqueta es una marca que se crea y se asigna a un AWS recurso de. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. También pueden ayudarlo a realizar un seguimiento de las acciones y las notificaciones de los propietarios de recursos. También puede usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS Recursos de etiquetado y la Guía del usuario de Tag Editor](#).

Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles desde muchos Servicios de AWS. No se han diseñado para usarse con información privada o confidencial.

Corrección

Para obtener información sobre cómo añadir etiquetas a una lista de EC2 prefijos de Amazon, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.177] las sesiones espejo EC2 de tráfico deberían estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::TrafficMirrorSession

Regla de AWS Config : [ec2-traffic-mirror-session-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Una lista de claves de etiquetas que no corresponden al sistema que deben asignarse a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una sesión duplicada de EC2 tráfico de Amazon tiene las claves de etiqueta especificadas por el `requiredKeyTags` parámetro. El control lanza error si la sesión no tiene ninguna clave de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no especifica ningún valor para el `requiredKeyTags` parámetro, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la sesión no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws:` prefijo.

Una etiqueta es una marca que se crea y se asigna a un AWS recurso de. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. También pueden ayudarlo a realizar un seguimiento de las acciones y las notificaciones de los propietarios de recursos. También puede usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS Recursos de etiquetado y la Guía del usuario de Tag Editor](#).

 Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles desde muchos Servicios de AWS. No se han diseñado para usarse con información privada o confidencial.

Corrección

Para obtener información sobre cómo añadir etiquetas a una sesión de Amazon EC2 Traffic Mirror, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.178] Los filtros espejo de EC2 tráfico deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::TrafficMirrorFilter

Regla de AWS Config : [ec2-traffic-mirror-filter-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Una lista de claves de etiquetas que no corresponden al sistema que deben asignarse a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un filtro espejo de EC2 tráfico de Amazon tiene las claves de etiqueta especificadas por el `requiredKeyTags` parámetro. El control lanza error si el filtro no tiene ninguna clave de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no especifica ningún valor para el `requiredKeyTags` parámetro, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el filtro no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws :` prefijo.

Una etiqueta es una marca que se crea y se asigna a un AWS recurso de. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. También pueden ayudarlo a realizar un seguimiento de las acciones y las notificaciones de los propietarios de recursos. También puede usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS Recursos de etiquetado y la Guía del usuario de Tag Editor](#).

Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles desde muchos Servicios de AWS. No se han diseñado para usarse con información privada o confidencial.

Corrección

Para obtener información sobre cómo añadir etiquetas a un filtro espejo de EC2 tráfico de Amazon, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.179] Los objetivos EC2 de tráfico reflejados deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EC2::TrafficMirrorTarget

Regla de AWS Config : [ec2-traffic-mirror-target-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Una lista de claves de etiquetas que no corresponden al sistema que deben asignarse a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un objetivo de EC2 tráfico duplicado de Amazon tiene las claves de etiqueta especificadas en el `requiredKeyTags` parámetro. El control lanza error si el objetivo no tiene ninguna clave de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no se especifica ningún valor para el `requiredKeyTags` parámetro, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el objetivo no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws:` prefijo.

Una etiqueta es una marca que se crea y se asigna a un AWS recurso de. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. También pueden ayudarlo a realizar un seguimiento de las acciones y las notificaciones de los propietarios de recursos. También puede usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS Recursos de etiquetado y la Guía del usuario de Tag Editor](#).

 Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles desde muchos Servicios de AWS. No se han diseñado para usarse con información privada o confidencial.

Corrección

Para obtener información sobre cómo añadir etiquetas a un objetivo espejo de EC2 tráfico de Amazon, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

Controles de Security Hub para el escalado automático

Estos controles de Security Hub evalúan el servicio y los recursos de Amazon EC2 Auto Scaling.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[AutoScaling.1] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar las comprobaciones de estado del ELB

Requisitos relacionados: PCI DSS v3.2.1/2.2, Nist.800-53.r5 CP-2 (2) NIST.800-53.r5 CA-7, Nist.800-53.r5 SI-2

Categoría: Identificar - Inventario

Gravedad: baja

Tipo de recurso: AWS::AutoScaling::AutoScalingGroup

Regla de AWS Config : [autoscaling-group-elb-healthcheck-required](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de Amazon EC2 Auto Scaling asociado a un balanceador de cargas utiliza comprobaciones de estado de Elastic Load Balancing (ELB). El control falla si el grupo de escalado automático no utiliza comprobaciones de estado de ELB.

Las comprobaciones de estado de ELB ayudan a garantizar que el grupo de escalado automático pueda determinar el estado de una instancia en función de las pruebas adicionales que proporciona el equilibrador de carga. El uso de comprobaciones de estado de Elastic Load Balancing también ayuda a respaldar la disponibilidad de las aplicaciones que utilizan grupos de EC2 Auto Scaling.

Corrección

Para añadir comprobaciones de estado de Elastic Load Balancing, consulte [Añadir comprobaciones de estado de Elastic Load Balancing](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

[AutoScaling.2] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::AutoScaling::AutoScalingGroup

Regla de AWS Config : [autoscaling-multiple-az](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
minAvailabilityZones	Cantidad mínima de zonas de disponibilidad	Enum	2, 3, 4, 5, 6	2

Este control comprueba si un grupo de Amazon EC2 Auto Scaling abarca al menos el número especificado de zonas de disponibilidad (AZs). El control falla si un grupo de Auto Scaling no abarca al menos el número especificado de AZs. A menos que proporciones un valor de parámetro personalizado para el número mínimo de AZs, Security Hub usa un valor predeterminado de dos AZs.

Un grupo de Auto Scaling que no abarque varias zonas no AZs puede lanzar instancias en otra zona de disponibilidad para compensar si la zona de disponibilidad única configurada deja de estar disponible. Sin embargo, en algunos casos de uso, puede preferirse un grupo de escalado automático con una sola zona de disponibilidad, como los trabajos por lotes o cuando los costos de transferencia entre zonas de disponibilidad deben mantenerse al mínimo. En esos casos, puede deshabilitar este control o suprimir sus resultados.

Corrección

Para añadir AZs a un grupo de Auto Scaling existente, consulte [Añadir y eliminar zonas de disponibilidad](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

[AutoScaling.3] Las configuraciones de lanzamiento de grupos de Auto Scaling deberían configurar las EC2 instancias para que requieran la versión 2 del Servicio de Metadatos de Instancia (IMDSv2)

Requisitos relacionados: NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, (7), NIST.800-53.r5 AC-3 NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 AC-6, NIST.800-53.r5 CM-2, PCI DSS v4.0.1/2.2.6

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: AWS::AutoScaling::LaunchConfiguration

Regla de AWS Config : [autoscaling-launchconfig-requires-imsdv2](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si IMDSv2 está activado en todas las instancias lanzadas por los grupos de Amazon EC2 Auto Scaling. El control falla si la versión del Instance Metadata Service (IMDS) no está incluida en la configuración de lanzamiento o si está configurada como `token optional`, que es una configuración que permite una IMDSv1 u IMDSv2 otra.

El IMDS brinda datos sobre una instancia que puede utilizar para configurar o administrar la instancia en ejecución.

La versión 2 del IMDS añade nuevas protecciones que no estaban disponibles IMDSv1 para proteger aún más las instancias EC2 .

Corrección

Un grupo de escalado automático asocia con una configuración de lanzamiento cada vez. No se puede modificar una configuración de lanzamiento después de crearla. Para cambiar la configuración de lanzamiento de un grupo de Auto Scaling, utilice una configuración de lanzamiento existente como base para una nueva configuración de lanzamiento con IMDSv2 Enabled. Para obtener más información, consulta [Configurar las opciones de metadatos de instancia para nuevas instancias](#) en la Guía del EC2 usuario de Amazon.

[AutoScaling.4] La configuración de inicio de grupos de Auto Scaling no debe tener un límite de saltos de respuesta de metadatos superior a 1

 Important

Security Hub retiró este control en abril de 2024. Para obtener más información, consulte [Registro de cambios para los controles CSPM de Security Hub](#).

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: AWS::AutoScaling::LaunchConfiguration

Regla de AWS Config : [autoscaling-launch-config-hop-limit](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba el número de saltos de red que puede recorrer un token de metadatos. El control falla si el límite de saltos de respuesta de los metadatos es superior a 1.

El Instance Metadata Service (IMDS) proporciona información de metadatos sobre una EC2 instancia de Amazon y es útil para la configuración de aplicaciones. Restringir la PUT respuesta HTTP del servicio de metadatos a solo la EC2 instancia protege al IMDS del uso no autorizado.

El campo Tiempo de vida (TTL) del paquete IP se reduce en uno en cada salto. Esta reducción se puede utilizar para garantizar que el paquete no viaje al exterior EC2. IMDSv2 protege EC2 las instancias que pueden estar mal configuradas como enrutadores abiertos, firewalls de capa 3, VPNs túneles o dispositivos NAT, lo que impide que los usuarios no autorizados recuperen los metadatos. Con IMDSv2, la PUT respuesta que contiene el token secreto no puede viajar fuera de la instancia porque el límite de saltos de respuesta de metadatos predeterminado está establecido en. 1 Sin embargo, si este valor es superior a1, el token puede salir de la EC2 instancia.

Corrección

Para modificar el límite de saltos de respuesta de metadatos para una configuración de lanzamiento existente, consulte [Modificar las opciones de metadatos de las instancias para las instancias existentes](#) en la Guía del EC2 usuario de Amazon.

[AutoScaling.5] EC2 Las instancias de Amazon lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas

Requisitos relacionados: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.4.4

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: AWS::AutoScaling::LaunchConfiguration

Regla de AWS Config : [autoscaling-launch-config-public-ip-disabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la configuración de lanzamiento asociada a un grupo de escalado automático asigna una [dirección IP pública](#) a las instancias del grupo. El control falla si la configuración de lanzamiento asociada asigna una dirección IP pública.

EC2 Las instancias de Amazon en una configuración de lanzamiento grupal de Auto Scaling no deben tener una dirección IP pública asociada, excepto en casos extremos limitados. Solo se debe poder acceder a las EC2 instancias de Amazon desde detrás de un balanceador de carga, en lugar de estar expuestas directamente a Internet.

Corrección

Un grupo de escalado automático asocia con una configuración de lanzamiento cada vez. No se puede modificar una configuración de lanzamiento después de crearla. Para cambiar la configuración de lanzamiento de un grupo de escalado automático, utilice una configuración de lanzamiento existente como punto de partida para una nueva configuración de lanzamiento. A continuación, actualice el grupo de escalado automático para utilizar la nueva configuración de lanzamiento. Para step-by-step obtener instrucciones, consulte [Cambiar la configuración de lanzamiento de un grupo de Auto Scaling](#) en la Guía del usuario de Amazon EC2 Auto Scaling. Al crear la nueva configuración de lanzamiento, en Configuración adicional, en Detalles avanzados, tipo de dirección IP, seleccione No asignar una dirección IP pública a ninguna instancia.

Después de cambiar la configuración de lanzamiento, Auto Scaling lanza nuevas instancias con las nuevas opciones de configuración. Las instancias existentes no se ven afectadas. Para actualizar una instancia existente, le recomendamos que actualice su instancia o permita que el escalado automático reemplace gradualmente las instancias más antiguas por instancias más recientes en función de sus políticas de terminación. Para obtener más información sobre la actualización de las instancias de Auto Scaling, consulte [Actualizar instancias de Auto Scaling](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

[AutoScaling.6] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::AutoScaling::AutoScalingGroup

Regla de AWS Config : [autoscaling-multiple-instance-types](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de Amazon EC2 Auto Scaling utiliza varios tipos de instancias. El control falla si el grupo de escalado automático solo tiene un tipo de instancia definido.

Puede mejorar la disponibilidad si implementa la aplicación en varios tipos de instancia que se ejecutan en varias zonas de disponibilidad. Security Hub recomienda utilizar varios tipos de instancias para que el grupo de escalado automático pueda lanzar otro tipo de instancia si no hay suficiente capacidad en las zonas de disponibilidad elegidas.

Corrección

Para crear un grupo de Auto Scaling con varios tipos de instancias, consulte [Grupos de Auto Scaling con varios tipos de instancias y opciones de compra](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

[AutoScaling.9] Los grupos de Amazon EC2 Auto Scaling deberían usar las plantillas de EC2 lanzamiento de Amazon

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoría: Identificar > Configuración de recursos

Gravedad: media

Tipo de recurso: AWS::AutoScaling::AutoScalingGroup

Regla de AWS Config : [autoscaling-launch-template](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si se ha creado un grupo de Amazon EC2 Auto Scaling a partir de una plantilla de EC2 lanzamiento. Este control falla si no se crea un grupo de Amazon EC2 Auto Scaling

con una plantilla de lanzamiento o si no se especifica una plantilla de lanzamiento en una política de instancias mixtas.

Se puede crear un grupo de EC2 Auto Scaling a partir de una plantilla de EC2 lanzamiento o una configuración de lanzamiento. Sin embargo, el uso de una plantilla de lanzamiento para crear un grupo de escalado automático garantiza que tenga acceso a las funciones y mejoras más recientes.

Corrección

Para crear un grupo de Auto Scaling con una plantilla de EC2 lanzamiento, consulte [Creación de un grupo de Auto Scaling mediante una plantilla de lanzamiento](#) en la Guía del usuario de Amazon EC2 Auto Scaling. Para obtener información sobre cómo reemplazar una configuración de lanzamiento por una plantilla de lanzamiento, consulta [Reemplazar una configuración de lanzamiento por una plantilla de lanzamiento](#) en la Guía del EC2 usuario de Amazon.

[AutoScaling.10] Los grupos EC2 de Auto Scaling deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::AutoScaling::AutoScalingGroup

Regla de AWS Config : tagged-autoscaling-autoscalinggroup (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un grupo de Amazon EC2 Auto Scaling tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el grupo de escalado automático no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el grupo de escalado automático no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un grupo de Auto Scaling, consulte [Etiquetar grupos e instancias de Auto Scaling](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

Controles de Security Hub para Amazon ECR

Estos controles de Security Hub evalúan el servicio y los recursos de Amazon Elastic Container Registry (Amazon ECR).

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[ECR.1] Los repositorios privados del ECR deben tener configurado el escaneo de imágenes

Requisitos relacionados: PCI DSS v4.0.1/6.2.3 NIST.800-53.r5 RA-5, PCI DSS v4.0.1/6.2.4

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: alta

Tipo de recurso: AWS::ECR::Repository

Regla de AWS Config : [ecr-private-image-scanning-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un repositorio privado de Amazon ECR tiene configurado el escaneo de imágenes. El control falla si el repositorio de ECR privado no está configurado para el escaneo instantáneo o continuo.

El escaneo de imágenes de ECR ayuda a identificar vulnerabilidades de software en las imágenes de contenedor. La configuración del escaneo de imágenes en los repositorios de ECR añade un nivel de verificación de la integridad y la seguridad de las imágenes que se almacenan.

Corrección

Para configurar el escaneo de imágenes para un repositorio de ECR, consulte el [Escaneo de imágenes](#) en la Guía del usuario de Amazon Elastic Container Registry.

[ECR.2] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas

Requisitos relacionados: (1), NiSt.800-53.r5 CM-2, NiSt.800-53.r5 CM-8 (1) NIST.800-53.r5 CA-9

Categoría: Identificar > Inventario > Etiquetado

Gravedad: media

Tipo de recurso: AWS::ECR::Repository

Regla de AWS Config : [ecr-private-tag-immutability-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un repositorio de ECR privado tiene habilitada la inmutabilidad de etiquetas. Este control falla si un repositorio de ECR privado tiene deshabilitada la inmutabilidad de etiquetas. Esta regla se aplica si la inmutabilidad de la etiqueta está habilitada y tiene el valor IMMUTABLE.

La inmutabilidad de las etiquetas ECR de Amazon permite a los clientes confiar en las etiquetas descriptivas de una imagen como un mecanismo fiable para rastrear e identificar las imágenes de forma única. Una etiqueta inmutable es estática, lo que significa que cada etiqueta hace referencia a una imagen única. Esto mejora la fiabilidad y la escalabilidad, ya que el uso de una etiqueta estática siempre tendrá como resultado la implementación de la misma imagen. Cuando se configura, la inmutabilidad de las etiquetas evita que se anulen, lo que reduce la superficie expuesta a ataques.

Corrección

Para crear un repositorio con etiquetas inmutables configuradas o para actualizar la configuración de mutabilidad de las etiquetas de imagen de un repositorio existente, consulte la [Mutabilidad de las etiquetas](#) de imagen en la Guía del usuario de Amazon Elastic Container registry.

[ECR.3] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NiSt.800-53.r5 CM-2, NiSt.800-53.r5 CM-2 (2)

Categoría: Identificar > Configuración de recursos

Gravedad: media

Tipo de recurso: AWS::ECR::Repository

Regla de AWS Config : [ecr-private-lifecycle-policy-configured](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un repositorio de Amazon ECR tiene configurada al menos una política de ciclo de vida. Este control falla si un repositorio de ECR no tiene ninguna política de ciclo de vida configurada.

Las políticas de ciclo de vida de Amazon ECR permiten especificar la administración de ciclo de vida de las imágenes de un repositorio. Al configurar las políticas del ciclo de vida, puede automatizar la limpieza de las imágenes sin utilizar y la caducidad de las imágenes en función de su antigüedad o recuento. La automatización de estas tareas puede ayudarte a evitar el uso involuntario de imágenes desactualizadas en tu repositorio.

Corrección

Para configurar una política de ciclo de vida, consulte la [Vista previa sobre cómo crear una política de ciclo de vida](#) en la Guía del usuario de Amazon Elastic Container Registry.

[ECR.4] Los repositorios públicos de ECR deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::ECR::PublicRepository

Regla de AWS Config : tagged-ecr-publicrepository (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un repositorio público de Amazon ECR tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el repositorio público no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el repositorio público no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un repositorio público de ECR, consulte [Tagging an Amazon ECR public repository](#) en la Guía del usuario de Amazon Elastic Container Registry.

[ECR.5] Los repositorios de ECR deben estar cifrados y gestionados por el cliente AWS KMS keys

Requisitos relacionados: NIST.800-53.r5 SC-1 2 (2), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 NIST.800-53.r5 CA-9 (6), NIST.800-53.r5 AU-9

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::ECR::Repository

Regla de AWS Config : [ecr-repository-cmk-encryption-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
kmsKeyArns	Una lista de los nombres de recursos de Amazon (ARNs) AWS KMS keys para incluirlos en la evaluación. El control genera una FAILED comprobación si un repositorio de ECR no está cifrado con una clave KMS de la lista.	StringList (máximo de 10 elementos)	De 1 a 10 ARNs de las claves KMS existentes. Por ejemplo: arn:aws:kms:us-west-2:11112223333:key/1234abcd-12ab-34cd-56ef-1234567890ab	Sin valor predeterminado

Este control comprueba si un repositorio de Amazon ECR está cifrado en reposo con un repositorio gestionado AWS KMS key por el cliente. El control falla si el repositorio de ECR no está cifrado con una clave KMS administrada por el cliente. Si lo desea, puede especificar una lista de claves de KMS para que el control las incluya en la evaluación.

De forma predeterminada, Amazon ECR cifra los datos del repositorio con claves administradas de Amazon S3 (SSE-S3) mediante un algoritmo AES-256. Para obtener un control adicional, puede

configurar Amazon ECR para que cifre los datos con un AWS KMS key (SSE-KMS o DSSE-KMS) en su lugar. La clave de KMS puede ser: una Clave administrada de AWS que Amazon ECR cree y administre para usted y que tenga el alias `aws/ecr`, o una clave administrada por el cliente que usted cree y administre en su Cuenta de AWS cuenta. Con una clave KMS administrada por el cliente, usted tiene el control total de la clave. Esto incluye definir y mantener la política de claves, administrar las concesiones, rotar el material criptográfico, asignar etiquetas, crear alias y habilitar y deshabilitar la clave.

 Note

AWS KMS admite el acceso multicuenta a las claves de KMS. Si un repositorio de ECR está cifrado con una clave KMS que pertenece a otra cuenta, este control no realiza comprobaciones entre cuentas al evaluar el repositorio. El control no evalúa si Amazon ECR puede acceder a la clave y utilizarla al realizar operaciones criptográficas para el repositorio.

Corrección

No puede cambiar la configuración de cifrado de un repositorio de ECR existente. Sin embargo, puede especificar una configuración de cifrado diferente para los repositorios de ECR que cree posteriormente. Amazon ECR admite el uso de diferentes configuraciones de cifrado para repositorios individuales.

Para obtener más información sobre las opciones de cifrado de los repositorios de ECR, consulte [Encryption at rest en](#) la Guía del usuario de Amazon ECR. Para obtener más información sobre la gestión por parte del cliente AWS KMS keys, consulte la AWS Key Management Service Guía para [AWS KMS keys](#) desarrolladores.

Controles de Security Hub para Amazon ECS

Estos controles de Security Hub evalúan el servicio y los recursos de Amazon Elastic Container Service (Amazon ECS). Es posible que los controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[ECS.1] Las definiciones de tareas de Amazon ECS deben tener modos de red seguros y definiciones de usuario

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6

Categoría: Proteger - Administración de acceso seguro

Gravedad: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regla de AWS Config : [ecs-task-definition-user-for-host-mode-check](#)

Tipo de horario: provocado por un cambio

Parámetros:

- `SkipInactiveTaskDefinitions: true` (no personalizable)

Este control comprueba si una definición de tarea de Amazon ECS activa con el modo de red de host tiene definiciones de contenedor de `privileged` o `user`. El control falla para definiciones de tarea que tienen modo de red host y definiciones de contenedor de `privileged=false`, vacío y `user=root`, o vacío.

Este control solo evalúa la última revisión activa de una definición de tarea de Amazon ECS.

El objetivo de este control es garantizar que el acceso se defina intencionalmente cuando se ejecutan tareas que utilizan el modo de red host. Si la definición de una tarea tiene privilegios elevados, es porque ha elegido esa configuración. Este control comprueba si hay una escalada inesperada de privilegios cuando la definición de una tarea tiene habilitada la red host y no se eligen privilegios elevados.

Corrección

Para obtener información sobre cómo actualizar una definición de tarea, consulte [Actualización de una definición de tarea](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

Al actualizar una definición de tarea, no se actualizan las tareas en ejecución que se iniciaron a partir de la definición de tarea anterior. Para actualizar una tarea en ejecución, debe volver a implementar la tarea con la nueva definición de tarea.

[ECS.2] Los servicios de ECS no deberían tener direcciones IP públicas asignadas automáticamente

Requisitos relacionados: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7,

NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: AWS::ECS::Service

Regla de AWS Config : `ecs-service-assign-public-ip-disabled` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los servicios de Amazon ECS están configurados para asignar direcciones IP públicas de forma automática. Este control tiene errores si `AssignPublicIP` figura como `ENABLED`. Este control se aprueba si `AssignPublicIP` figura como `DISABLED`.

Una dirección IP pública es una dirección IP a la que se puede tener acceso desde Internet. Si lanza sus instancias de Amazon ECS con una dirección IP pública, podrá acceder a sus instancias de Amazon ECS desde Internet. Los servicios de Amazon ECS no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a los servidores de aplicaciones contenedoras.

Corrección

En primer lugar, debe crear una definición de tareas para el clúster que utilice el modo de red `awsvpc` y especifique `FARGATE` para `requiresCompatibilities`. A continuación, para la configuración de cómputo, elija el Tipo de lanzamiento y `FARGATE`. Por último, en el campo Redes, desactive la IP pública para deshabilitar la asignación automática de IP pública para su servicio.

[ECS.3] Las definiciones de tareas de ECS no deben compartir el espacio de nombres de los procesos del anfitrión

Requisitos relacionados: (1), NIST.800-53.r5 CM-2 NIST.800-53.r5 CA-9

Categoría: Identificar > Configuración de recursos

Gravedad: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regla de AWS Config : [ecs-task-definition-pid-mode-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las definiciones de tareas de Amazon ECS están configuradas para compartir el espacio de nombres de procesos de un host con sus contenedores. El control falla si la definición de la tarea comparte el espacio de nombres del proceso del host con los contenedores que se ejecutan en él. Este control solo evalúa la última revisión activa de una definición de tarea de Amazon ECS.

Un espacio de nombres de ID de proceso (PID) proporciona separación entre los procesos. Evita que los procesos del sistema sean visibles y permite PIDs su reutilización, incluido el PID 1. Si el espacio de nombres PID del host se comparte con los contenedores, los contenedores podrían ver todos los procesos del sistema anfitrión. Esto reduce la ventaja del aislamiento a nivel de proceso entre el host y los contenedores. Estas circunstancias podrían provocar el acceso no autorizado a los procesos del propio host, incluida la posibilidad de manipularlos y cancelarlos. Los clientes no deberían compartir el espacio de nombres de los procesos del anfitrión con los contenedores que se ejecuten en él.

Corrección

Para configurar el `pidMode` de la definición de una tarea, consulte [Parámetros de definición de tareas](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.4] Los contenedores de ECS deben ejecutarse sin privilegios

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6

Categoría: Proteger > Gestión del acceso seguro > Restricciones de acceso para los usuarios raíz

Gravedad: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regla de AWS Config : [ecs-containers-nonprivileged](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el parámetro `privileged` de la definición de contenedor de las definiciones de tareas de Amazon ECS se establece como `true`. El control falla si este parámetro es igual a `true`. Este control solo evalúa la última revisión activa de una definición de tarea de Amazon ECS.

Le recomendamos que elimine los privilegios elevados de las definiciones de tareas de ECS. Cuando el parámetro de privilegio es `true`, al contenedor se le conceden privilegios elevados en la instancia de contenedor de host (similares a los de un usuario raíz).

Corrección

Para configurar el parámetro `privileged` en una definición de tarea, consulte [Parámetros de definición avanzada de contenedor](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.5] Los contenedores ECS deben limitarse al acceso de solo lectura a los sistemas de archivos raíz

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Categoría: Proteger - Administración de acceso seguro

Gravedad: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regla de AWS Config : [ecs-containers-readonly-access](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un contenedor de Amazon ECS tiene acceso de solo lectura a su sistema de archivos raíz. El control falla si el `readonlyRootFilesystem` parámetro está establecido en `false`, o si el parámetro no existe en la definición del contenedor dentro de la definición de la tarea. Este control evalúa solo la última revisión activa de una definición de tarea de Amazon ECS.

Si el `readonlyRootFilesystem` parámetro se establece `true` en una definición de tarea de Amazon ECS, el contenedor de ECS tiene acceso de solo lectura a su sistema de archivos raíz. Esto reduce los vectores de ataque a la seguridad, ya que no se puede manipular ni escribir en el sistema de archivos raíz de la instancia contenedora sin montajes de volumen explícitos que tengan permisos de lectura y escritura para las carpetas y directorios del sistema de archivos. Al habilitar esta opción también se sigue el principio de privilegios mínimos.

Corrección

Para conceder a un contenedor de Amazon ECS acceso de solo lectura a su sistema de archivos raíz, añada el `readonlyRootFilesystem` parámetro a la definición de tarea del contenedor y establezca el valor del parámetro en `true`. Para obtener información sobre los parámetros de definición de tareas y cómo añadirlos a una definición de tarea, consulte [Definiciones de tareas de Amazon ECS](#) y [Actualización de una definición de tarea](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.8] Los secretos no deben pasarse como variables de entorno del contenedor

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, PCI DSS v4.0.1/8.6.2

Categoría: Proteger > Desarrollo seguro > Credenciales no codificadas

Gravedad: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regla de AWS Config : [ecs-no-environment-secrets](#)

Tipo de horario: provocado por un cambio

AWS_SECRET_ACCESS_KEY Parámetros `secretKeys`: `AWS_ACCESS_KEY_ID`
`ECS_ENGINE_AUTH_DATA` (no personalizables)

Este control comprueba si el valor clave de alguna variable del parámetro `environment` de las definiciones de contenedores incluye `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY`, o `ECS_ENGINE_AUTH_DATA`. Este control falla si una sola variable de entorno en cualquier definición de contenedor es igual a `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY`, o `ECS_ENGINE_AUTH_DATA`. Este control no cubre las variables de entorno que se transmiten desde otras ubicaciones, como Amazon S3. Este control solo evalúa la última revisión activa de una definición de tarea de Amazon ECS.

AWS Systems Manager Parameter Store puede ayudarlo a mejorar la postura de seguridad de su organización. Le recomendamos que utilice el almacén de parámetros para almacenar los secretos y las credenciales en lugar de pasarlos directamente a las instancias contenedoras o codificarlos en el código.

Corrección

Para crear parámetros mediante SSM, consulte [Creación de parámetros de Systems Manager](#) en la Guía del usuario de AWS Systems Manager . Para obtener más información sobre cómo crear una definición de tarea que especifique un secreto, consulte [Especificar datos confidenciales mediante Secrets Manager](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.9] Las definiciones de tareas de ECS deben tener una configuración de registro

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: alta

Tipo de recurso: AWS::ECS::TaskDefinition

AWS Config regla `ecs-task-definition-log` -configuración

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la última definición de tarea activa de Amazon ECS tiene una configuración de registro especificada. El control falla si la definición de la tarea no tiene la propiedad definida `logConfiguration` o si el valor `logDriver` es null en al menos una definición de contenedor.

El registro le ayuda a mantener la fiabilidad, la disponibilidad y el rendimiento de Amazon ECS. La recopilación de datos de las definiciones de tareas proporciona visibilidad, lo que puede ayudarlo a depurar los procesos y encontrar la causa raíz de los errores. Si utiliza una solución de registro que no tiene que estar definida en la definición de tareas de ECS (como una solución de registro de terceros), puede deshabilitar este control después de asegurarse de que los registros se capturan y entregan correctamente.

Corrección

Para definir una configuración de registro para las definiciones de tareas de Amazon ECS, consulte [Especificación de una configuración de registro en la definición de tareas](#) de la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.10] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate

Requisitos relacionados: niST.800-53.r5 SI-2, niST.800-53.r5 SI-2 (2), niST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: media

Tipo de recurso: AWS::ECS::Service

Regla de AWS Config : [ecs-fargate-latest-platform-version](#)

Tipo de horario: provocado por un cambio

Parámetros:

- latestLinuxVersion: 1.4.0 (no personalizable)
- latestWindowsVersion: 1.0.0 (no personalizable)

Este control comprueba si los servicios Fargate de Amazon ECS ejecutan la versión más reciente de la versión de la plataforma Fargate. Este control falla si la versión de la plataforma no es la más reciente.

AWS Fargate las versiones de plataforma se refieren a un entorno de ejecución específico para la infraestructura de tareas de Fargate, que es una combinación de versiones de ejecución de kernel y contenedor. Se lanzan nuevas versiones de la plataforma a medida que evoluciona el tiempo de ejecución. Por ejemplo, se puede lanzar una nueva versión de kernel o del sistema operativo, características nuevas, correcciones de errores o actualizaciones de seguridad. Las actualizaciones y los parches de seguridad se implementan automáticamente para las tareas de Fargate. Si se detecta un problema de seguridad que afecte a una versión de la plataforma, corrija AWS la versión de la plataforma.

Corrección

Para actualizar un servicio existente, incluida su versión de la plataforma, consulte [Actualización de un servicio](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.12] Los clústeres de ECS deben usar Container Insights

Requisitos relacionados: NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7
NIST.800-53.r5 SI-2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::ECS::Cluster

Regla de AWS Config : [ecs-container-insights-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los clústeres de ECS utilizan Container Insights. Este control falla si Container Insights no está configurado para un clúster.

La monitorización es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de los clústeres de Amazon ECS. Utilice CloudWatch Container Insights para recopilar, agregar y resumir las métricas y los registros de sus aplicaciones y microservicios contenerizados. CloudWatch recopila automáticamente las métricas de muchos recursos, como la CPU, la memoria, el disco y la red. Información de contenedores también proporciona información de diagnóstico, como, por ejemplo, errores de reinicio de contenedores, para ayudarlo a aislar problemas y solucionarlos rápidamente. También puedes configurar CloudWatch alarmas en las métricas que recopila Container Insights.

Corrección

Para usar Container Insights, consulta [Actualización de un servicio](#) en la Guía del CloudWatch usuario de Amazon.

[ECS.13] Los servicios de ECS deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::ECS::Service`

Regla de AWS Config : `tagged-ecs-service` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un servicio de Amazon ECS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el servicio no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el servicio no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un servicio de ECS, consulte [Etiquetado de los recursos de Amazon ECS](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.14] Los clústeres de ECS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::ECS::Cluster`

Regla de AWS Config : `tagged-ecs-cluster` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un clúster de Amazon ECS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el clúster no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el clúster no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un clúster de ECS, consulte [Etiquetado de los recursos de Amazon ECS](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.15] Las definiciones de tareas de ECS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::ECS::TaskDefinition`

Regla de AWS Config : tagged-ecs-taskdefinition (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una definición de tarea de Amazon ECS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si la definición de la tarea no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si la definición de la tarea no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una definición de tarea de ECS, consulte [Etiquetado de los recursos de Amazon ECS](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.16] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas

Requisitos relacionados: PCI DSS v4.0.1/1.4.4

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: AWS::ECS::TaskSet

Regla de AWS Config : `ecs-taskset-assign-public-ip-disabled` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los conjuntos de tareas de Amazon ECS están configurados para asignar direcciones IP públicas de forma automática. El control tiene errores si `AssignPublicIP` está configurado como `ENABLED`,

Una dirección IP pública es una dirección a la que se puede tener acceso desde Internet. Si configura el conjunto de tareas con una dirección IP pública, se puede acceder a los recursos asociados al conjunto de tareas desde Internet. Los conjuntos de tareas de ECS no deben ser de acceso público, ya que esto podría permitir el acceso no deseado a los servidores de aplicaciones contenedoras.

Corrección

Para actualizar un conjunto de tareas de ECS para que no utilice una dirección IP pública, consulte [Actualización de una definición de tareas de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.17] Las definiciones de tareas de ECS no deben utilizar el modo de red host

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3 (15),, NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: AWS::ECS::TaskDefinition

Regla de AWS Config : [ecs-task-definition-network-mode-not-host](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la última revisión activa de una definición de tarea de Amazon ECS utiliza el modo host de red. El control falla si la última revisión activa de la definición de tarea de ECS utiliza el modo host de red.

Cuando se utiliza el modo de host red, la red de un contenedor de Amazon ECS está vinculada directamente al host subyacente que ejecuta el contenedor. Por lo tanto, este modo permite que los contenedores se conecten a los servicios de red de bucle invertido privados del host y se hagan pasar por el anfitrión. Otros inconvenientes importantes son que no se puede reasignar un puerto de contenedor cuando se utiliza el modo de host red y no se puede ejecutar más de una sola instancia de una tarea en cada host.

Corrección

Para obtener información sobre los modos y opciones de red para las tareas de Amazon ECS que se alojan en las EC2 instancias de Amazon, consulte [las opciones de redes de tareas de Amazon ECS para el tipo de EC2 lanzamiento](#) en la Guía para desarrolladores de Amazon Elastic Container Service. Para obtener información sobre cómo crear una nueva revisión de una definición de tarea y especificar un modo de red diferente, consulte [Actualización de una definición de tarea de Amazon ECS](#) en esa guía.

Si la definición de tarea de Amazon ECS la creó AWS Batch, consulte [Modos de red para AWS Batch trabajos para](#) obtener información sobre los modos de red y el uso típico de los tipos de AWS Batch trabajo y para elegir una opción segura.

Controles de Security Hub para Amazon EFS

Estos controles de Security Hub evalúan el servicio y los recursos de Amazon Elastic File System (Amazon EFS).

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[EFS.1] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.4.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SC-2 NIST.800-53.r5 SI-7 (6) NIST.800-53.r5 SC-7

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::EFS::FileSystem

Regla de AWS Config : [efs-encrypted-check](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si Amazon Elastic File System está configurado para cifrar los datos del archivo mediante AWS KMS. La comprobación falla en los siguientes casos.

- Encrypted se establece en false en la respuesta de [DescribeFileSystems](#).
- La clave KmsKeyId de la respuesta de [DescribeFileSystems](#) no coincide con el parámetro KmsKeyId de [efs-encrypted-check](#).

Tenga en cuenta que este control no utiliza el parámetro KmsKeyId para [efs-encrypted-check](#). Solo comprueba el valor de Encrypted.

Para añadir un nivel de seguridad a sus datos confidenciales en Amazon EFS, debe crear sistemas de archivos cifrados. Amazon EFS admite el cifrado de sistemas de archivos en reposo. Puede habilitar el cifrado de datos en reposo cuando cree un sistema de archivos de Amazon EFS. Para obtener más información acerca del cifrado de Amazon EFS, consulte [Cifrado de datos en Amazon EFS](#) en la Guía del usuario de Amazon Elastic File System.

Corrección

Para obtener información detallada sobre cómo cifrar un nuevo sistema de archivos de Amazon EFS, consulte [Cifrado de datos en reposo](#) en la Guía del usuario de Amazon Elastic File System.

[EFS.2] Los volúmenes de Amazon EFS deben estar en los planes de respaldo

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Backup

Gravedad: media

Tipo de recurso: AWS::EFS::FileSystem

Regla de AWS Config : [efs-in-backup-plan](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si los sistemas de archivos de Amazon Elastic File System (Amazon EFS) se han agregado a los planes de copia de seguridad en AWS Backup. El control falla si los sistemas de archivos Amazon EFS no están incluidos en los planes de backup.

La inclusión de los sistemas de archivos EFS en los planes de copia de seguridad le ayuda a proteger sus datos contra la eliminación y la pérdida de datos.

Corrección

Para habilitar las copias de seguridad automáticas para un sistema de archivos Amazon EFS existente, consulte [Introducción 4: Creación de copias de seguridad automáticas de Amazon EFS](#) en la Guía para desarrolladores de AWS Backup .

[EFS.3] Los puntos de acceso EFS deben aplicar un directorio raíz

Requisitos relacionados: NIST.800-53.r5 AC-6 (10)

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS::EFS::AccessPoint

Regla de AWS Config : [efs-access-point-enforce-root-directory](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los puntos de acceso de Amazon EFS están configurados para aplicar un directorio raíz. El control falla si el valor Path se establece como / (el directorio raíz predeterminado del sistema de archivos).

Cuando se aplica un directorio raíz, el cliente NFS que utiliza el punto de acceso utiliza el directorio raíz configurado en el punto de acceso en lugar del directorio raíz del sistema de archivos. La aplicación de un directorio raíz para un punto de acceso ayuda a restringir el acceso a los datos, ya que garantiza que los usuarios del punto de acceso solo puedan acceder a los archivos del subdirectorio especificado.

Corrección

Para obtener instrucciones sobre cómo aplicar un directorio raíz para un punto de acceso de Amazon EFS, consulte [Aplicación de un directorio raíz con un punto de acceso](#) en la Guía del usuario de Amazon Elastic File System.

[EFS.4] Los puntos de acceso EFS deben imponer una identidad de usuario

Requisitos relacionados: NIST.800-53.r5 AC-6 (2), PCI DSS v4.0.1/7.3.1

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS::EFS::AccessPoint

Regla de AWS Config : [efs-access-point-enforce-user-identity](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los puntos de acceso de Amazon EFS están configurados para imponer la identidad de un usuario. Este control falla si no se define una identidad de usuario POSIX al crear el punto de acceso EFS.

Los puntos de acceso de Amazon EFS son puntos de entrada específicos que la aplicación utiliza para acceder a un sistema de archivos de EFS y que facilitan la administración del acceso de las aplicaciones a conjuntos de datos compartidos. Los puntos de acceso pueden imponer una identidad de usuario, incluidos los grupos POSIX del usuario, para todas las solicitudes del sistema de archivos que se realizan a través del punto de acceso. Los puntos de acceso también pueden imponer un directorio raíz diferente para el sistema de archivos, de modo que los clientes solo puedan acceder a los datos del directorio especificado o de sus subdirectorios.

Corrección

Para hacer cumplir la identidad de un usuario para un punto de acceso de Amazon EFS, consulte [Imponer una identidad de usuario mediante un punto de acceso](#) en la Guía del usuario de Amazon Elastic File System.

[EFS.5] Los puntos de acceso de EFS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EFS::AccessPoint

Regla de AWS Config: tagged-efs-accesspoint (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un punto de acceso de Amazon EFS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el punto de acceso no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el punto de acceso no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre

ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un punto de acceso de EFS, consulte [Tagging Amazon EFS resources](#) en la Guía del usuario de Amazon Elastic File System.

[EFS.6] Los destinos de montaje de EFS no deben estar asociados a una subred pública

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: media

Tipo de recurso: AWS::EFS::FileSystem

Regla de AWS Config : [efs-mount-target-public-accessible](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un destino de montaje de Amazon EFS está asociado a una subred privada. El control lanza error si el destino de montaje está asociado a una subred pública.

De forma predeterminada, solo se puede acceder a un sistema de archivos desde la nube privada virtual (VPC) en la que se creó. Recomendamos crear destinos de montaje de EFS en subredes privadas a las que no se pueda acceder desde Internet. Esto ayuda a garantizar que solo los usuarios autorizados puedan acceder a su sistema de archivos y que este no sea vulnerable a ataques o accesos no autorizados.

Corrección

No puede cambiar la asociación entre un destino de montaje de EFS y una subred después de crear el destino de montaje. Para asociar un destino de montaje existente a una subred diferente, debe crear un destino de montaje nuevo en una subred privada y luego, eliminar el destino de montaje anterior. Para obtener información acerca de la administración de destinos de montaje, consulte

[Creación y administración de destinos de montaje y grupos de seguridad](#) en la Guía del usuario de Amazon Elastic File System.

[EFS.7] Los sistemas de archivos de EFS deben tener habilitadas las copias de seguridad automáticas

Gravedad: media

Tipo de recurso: AWS::EFS::FileSystem

Regla de AWS Config : [efs-automatic-backups-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un sistema de archivos de Amazon EFS tiene habilitadas las copias de seguridad automáticas. Este control lanza error si el sistema de archivos de EFS no tiene habilitadas las copias de seguridad automáticas.

Una copia de seguridad de datos es una copia de los datos del sistema, la configuración o la aplicación que se almacena por separado del original. La habilitación de copias de seguridad periódicas ayuda a proteger los datos valiosos frente a eventos imprevistos, como errores del sistema, ciberataques o eliminaciones accidentales. Contar con una estrategia de copia de seguridad sólida también permite una recuperación más rápida, una continuidad empresarial y brinda tranquilidad frente a una posible pérdida de datos.

Corrección

Para obtener información sobre el uso AWS Backup de los sistemas de archivos EFS, consulte [Cómo hacer copias de seguridad de los sistemas de archivos EFS](#) en la Guía del usuario de Amazon Elastic File System

[EFS.8] Los sistemas de archivos de EFS deben cifrarse en reposo

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::EFS::FileSystem

Regla de AWS Config : [efs-filessystem-ct-encrypted](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un sistema de archivos Amazon EFS cifra los datos con AWS Key Management Service (AWS KMS). El control lanza error si un sistema de archivos no está cifrado.

Los datos en reposo hacen referencia a los datos que se almacenan en un almacenamiento persistente y no volátil durante cualquier periodo de tiempo. El cifrado de datos en reposo permite proteger la confidencialidad de los datos, lo que reduce el riesgo de que un usuario no autorizado pueda acceder a ellos.

Corrección

Para habilitar el cifrado en reposo para un sistema de archivos de EFS nuevo, consulte [Cifrado de datos en reposo](#) en la Guía del usuario de Amazon Elastic File System.

Controles de Security Hub para Amazon EKS

Estos controles de Security Hub evalúan el servicio Amazon Elastic Kubernetes Service (Amazon EKS) y sus recursos. Es posible que los controles no estén disponibles en todos. Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[EKS.1] Los puntos de enlace del clúster EKS no deben ser de acceso público

Requisitos relacionados: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: AWS::EKS::Cluster

Regla de AWS Config : [eks-endpoint-no-public-access](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un punto de conexión de un clúster de Amazon EKS es de acceso público. El control falla si un clúster de EKS tiene un punto de conexión al que se puede acceder públicamente.

Cuando crea un clúster nuevo, Amazon EKS genera un punto de conexión para el servidor de la API de Kubernetes administrado que utiliza a fin de comunicarse con su clúster. De forma predeterminada, este punto de conexión del servidor API está disponible públicamente en Internet. El acceso al servidor API está protegido mediante una combinación de AWS Identity and Access Management (IAM) y el control de acceso basado en roles (RBAC) nativo de Kubernetes. Al eliminar el acceso público al punto de conexión, puede evitar la exposición y el acceso involuntarios a su clúster.

Corrección

Para modificar el acceso a los puntos de conexión de un clúster de EKS existente, consulte [Modificación del acceso a los puntos de conexión de un clúster](#) en la Guía del usuario de Amazon EKS. Puede configurar el acceso a los puntos de conexión para un nuevo clúster de EKS al crearlo. Para obtener instrucciones sobre cómo crear un nuevo clúster de Amazon EKS, consulte [Creación de un clúster de Amazon EKS](#) en la Guía del usuario de Amazon EKS.

[EKS.2] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NiSt.800-53.r5 CM-2, NiSt.800-53.r5 SI-2, NiSt.800-53.r5 SI-2 (2), NiSt.800-53.r5 SI-2 (4), NiSt.800-53.r5 SI-2 (5), PCI DSS v4.0.1/12.3.4

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: alta

Tipo de recurso: AWS::EKS::Cluster

Regla de AWS Config : [eks-cluster-supported-version](#)

Tipo de horario: provocado por un cambio

Parámetros:

- `oldestVersionSupported: 1.30` (no personalizable)

Este control comprueba si un clúster de Amazon Elastic Kubernetes Service (Amazon EKS) se ejecuta en una versión de Kubernetes compatible. El control lanza un error si el clúster de EKS se ejecuta en una versión no compatible.

Si su aplicación no requiere una versión específica de Kubernetes, recomendamos que use la versión más reciente de Kubernetes disponible admitida por EKS para sus clústeres. Para obtener más información, consulte el [calendario de lanzamientos de Amazon EKS Kubernetes](#) y [Conozca el ciclo de vida de las versiones de Kubernetes en Amazon EKS en la Guía del usuario de Amazon EKS](#).

Corrección

Para actualizar un clúster de EKS, consulte [Actualizar un clúster existente a una nueva versión de Kubernetes en la Guía del usuario](#) de Amazon EKS.

[EKS.3] Los clústeres de EKS deben usar secretos de Kubernetes cifrados

Requisitos relacionados: NIST.800-53.r5 SC-1 2 NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-1 3, 8, PCI DSS NIST.800-53.r5 SC-2 v4.0.1/8.3.2

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::EKS::Cluster

Regla de AWS Config : [eks-cluster-secrets-encrypted](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un clúster de Amazon EKS utiliza secretos de Kubernetes cifrados. El control lanza un error si los secretos de Kubernetes del clúster no están cifrados.

Al cifrar los secretos, puede utilizar las claves AWS Key Management Service (AWS KMS) para cifrar en sobres los secretos de Kubernetes almacenados en etcd para su clúster. Este cifrado se suma al cifrado de volúmenes de EBS, que está habilitado de forma predeterminada para todos los datos (incluidos los secretos) que se almacenan en etcd como parte de un clúster de EKS. El uso del cifrado de secretos para su clúster de EKS le permite implementar una estrategia de defensa exhaustiva para las aplicaciones de Kubernetes mediante el cifrado de los secretos de Kubernetes con una clave de KMS que usted defina y administre.

Corrección

Para habilitar el cifrado de secretos en un clúster de EKS, consulte [Habilitar el cifrado de secretos en un clúster existente](#) en la Guía del usuario de Amazon EKS.

[EKS.6] Los clústeres de EKS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::EKS::Cluster`

Regla de AWS Config : `tagged-eks-cluster` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un clúster de Amazon EKS tiene etiquetas con claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el clúster no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el clúster no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno

u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un clúster de EKS, consulte [Etiquetado de los recursos de Amazon EKS](#) en la Guía del usuario de Amazon EKS.

[EKS.7] Las configuraciones de los proveedores de identidad de EKS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::EKS::IdentityProviderConfig

Regla de AWS Config : tagged-eks-identityproviderconfig (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una configuración de los proveedores de identidad de Amazon EKS tiene etiquetas con claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la configuración no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la configuración no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre

ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a las configuraciones de los proveedores de identidad de EKS, consulte [Etiquetado de los recursos de Amazon EKS](#) en la Guía del usuario de Amazon EKS.

[EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), (4), NIST.800-53.r5 AC-2 (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::EKS::Cluster

Regla de AWS Config : [eks-cluster-log-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros:

- logTypes: audit (no personalizable)

Este control comprueba si un clúster de Amazon EKS tiene habilitado el registro de auditoría. Se produce un error en el control si el registro de auditoría no está habilitado para el clúster.

Note

Este control no comprueba si el registro de auditoría de Amazon EKS está habilitado a través de Amazon Security Lake para la Cuenta de AWS.

El registro del plano de control de EKS proporciona registros de auditoría y diagnóstico directamente desde el plano de control de EKS a Amazon CloudWatch Logs de su cuenta. Puede seleccionar los tipos de registro que necesita y los registros se envían como flujos de registros a un grupo por cada clúster de EKS en el que se encuentre CloudWatch. El registro proporciona visibilidad del acceso y el rendimiento de los clústeres de EKS. Al enviar los registros del plano de control de EKS para sus clústeres de EKS a CloudWatch Logs, puede registrar las operaciones con fines de auditoría y diagnóstico en una ubicación central.

Corrección

Para habilitar los registros de auditoría para el clúster de EKS, consulte [Habilitación y deshabilitación de registros de plano de control](#) en la Guía del usuario de Amazon EKS.

Controles de Security Hub para ElastiCache

Estos AWS Security Hub controles evalúan el ElastiCache servicio y los recursos de Amazon.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[ElastiCache.1] Los clústeres ElastiCache (Redis OSS) deben tener habilitadas las copias de seguridad automáticas

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: alta

Tipo de recurso: AWS::ElastiCache::CacheCluster,
AWS:ElastiCache:ReplicationGroup

Regla de AWS Config : [elasticache-redis-cluster-automatic-backup-check](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
snapshotRetentionPeriod	Periodo mínimo de retención de instantáneas en días	Entero	De 1 a 35	1

Este control evalúa si un clúster de Amazon ElastiCache (Redis OSS) tiene copias de seguridad automáticas programadas. Se produce un error en el control si el valor de `SnapshotRetentionLimit` del clúster de Redis es inferior al periodo especificado. A menos que se proporcione un valor personalizado de parámetro para el periodo de retención de instantáneas, Security Hub utiliza un valor predeterminado de 1 día.

Los clústeres de Amazon ElastiCache (Redis OSS) pueden hacer copias de seguridad de sus datos. Puede utilizar la característica de copia de seguridad para restaurar un clúster o para propagar datos en un nuevo clúster. La copia de seguridad se compone de los metadatos del clúster, junto con todos los datos del clúster. Todas las copias de seguridad se escriben en Amazon Simple Storage Service (Amazon S3), lo que proporciona un almacenamiento duradero. Puede restaurar los datos creando un nuevo clúster de Redis y rellenándolo con los datos de una copia de seguridad. Puede gestionar las copias de seguridad mediante AWS Management Console, AWS Command Line Interface (AWS CLI) y la ElastiCache API.

Corrección

Para programar copias de seguridad automáticas en un clúster ElastiCache (Redis OSS), consulte [Programar copias de seguridad automáticas](#) en la Guía del ElastiCache usuario de Amazon.

[ElastiCache.2] ElastiCache Los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias

Requisitos relacionados: NIST.800-53.r5 SI-2, niST.800-53.r5 SI-2 (2), niST.800-53.r5 SI-2 (4), Nist.800-53.r5 SI-2 (5) PCI DSS v4.0.1/6.3.3

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: alta

Tipo de recurso: AWS::ElastiCache::CacheCluster

Regla de AWS Config : [elasticache-auto-minor-version-upgrade-check](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control evalúa si Amazon aplica ElastiCache automáticamente las actualizaciones de versiones menores a un clúster de caché. El control falla si no se aplican automáticamente las actualizaciones de versiones menores del clúster de caché.

 Note

Este control no se aplica a los clústeres de ElastiCache Memcached.

La actualización automática de versiones secundarias es una función que puedes activar en Amazon ElastiCache para actualizar automáticamente tus clústeres de caché cuando haya disponible una nueva versión del motor de caché secundaria. Estas actualizaciones pueden incluir parches de seguridad y correcciones de errores. Seguir up-to-date con la instalación de los parches es un paso importante para proteger los sistemas.

Corrección

Para aplicar automáticamente actualizaciones de versiones menores a un clúster de ElastiCache caché existente, consulte [Gestión de versiones ElastiCache](#) en la Guía del ElastiCache usuario de Amazon.

[ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::ElastiCache::ReplicationGroup

Regla de AWS Config : [elasticache-repl-grp-auto-failover-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un grupo de replicación tiene habilitada la conmutación por error automática. El control falla si la conmutación por error automática no está habilitada para un grupo de replicación.

Cuando se habilita la conmutación por error automática para un grupo de replicación, la característica del nodo principal tendrá una conmutación por error automática en una de las réplicas de lectura. Esta conmutación por error y promoción de réplica garantizan que pueda reanudar la escritura en la réplica principal tan pronto como se complete la promoción, lo cual reduce el tiempo de inactividad general en caso de falla.

Corrección

Para habilitar la conmutación por error automática para un grupo de ElastiCache replicación existente, consulte [Modificación de un ElastiCache clúster](#) en la Guía del ElastiCache usuario de Amazon. Si utiliza la ElastiCache consola, active la conmutación por error automática.

[ElastiCache.4] los grupos de ElastiCache replicación deben estar cifrados en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::ElastiCache::ReplicationGroup

Regla de AWS Config : [elasticache-repl-grp-encrypted-at-rest](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un grupo de ElastiCache replicación está cifrado en reposo. El control produce un error si el grupo de replicación no está cifrado en reposo.

El cifrado de los datos en reposo reduce el riesgo de que un usuario no autenticado acceda a los datos almacenados en el disco. ElastiCache Los grupos de replicación (Redis OSS) deben cifrarse en reposo para ofrecer un nivel de seguridad adicional.

Corrección

Para configurar el cifrado en reposo en un grupo de ElastiCache replicación, consulte [Habilitar el cifrado en reposo](#) en la Guía ElastiCache del usuario de Amazon.

[ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3 (3), (NIST.800-53.r5 SC-13), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), PCI DSS v4.0.1/4.2.1

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::ElastiCache::ReplicationGroup

Regla de AWS Config : [elasticache-repl-grp-encrypted-in-transit](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un grupo de ElastiCache replicación está cifrado en tránsito. El control falla si el grupo de replicación no está cifrado en tránsito.

El cifrado de los datos en tránsito reduce el riesgo de que un usuario no autorizado pueda espiar el tráfico de la red. Al habilitar el cifrado en tránsito en un grupo de ElastiCache replicación, se cifran los datos siempre que se mueven de un lugar a otro, por ejemplo, entre los nodos del clúster o entre el clúster y la aplicación.

Corrección

Para configurar el cifrado en tránsito en un grupo de ElastiCache replicación, consulte [Habilitar el cifrado en tránsito](#) en la Guía ElastiCache del usuario de Amazon.

[ElastiCache.6] Los grupos de replicación ElastiCache (Redis OSS) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 (7), PCI DSS v4.0.1/8.3.1 NIST.800-53.r5 AC-6

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS::ElastiCache::ReplicationGroup

Regla de AWS Config : [elasticache-repl-grp-redis-auth-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un grupo de replicación ElastiCache (Redis OSS) tiene habilitada la autenticación de Redis OSS. Se produce un error en el control si la versión de Redis OSS de los nodos del grupo de replicación es inferior a la 6.0 y AuthToken no está en uso.

Cuando utiliza los tokens de autenticación o contraseñas de Redis, Redis solicita una contraseña antes de permitir que los clientes ejecuten comandos, lo cual mejora la seguridad de los datos. Para Redis 6.0 y versiones posteriores, se recomienda utilizar el control de acceso basado en roles (RBAC). Como el RBAC no es compatible con las versiones de Redis anteriores a la 6.0, este control solo evalúa las versiones que no pueden usar la característica RBAC.

Corrección

Para usar Redis AUTH en un grupo de replicación ElastiCache (Redis OSS), consulte [Modificación del token AUTH en un clúster existente ElastiCache \(Redis OSS\) en](#) la Guía del usuario de Amazon. ElastiCache

[ElastiCache.7] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado

Requisitos relacionados: NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: AWS::ElasticCache::CacheCluster

Regla de AWS Config : [elasticache-subnet-group-check](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un ElasticCache clúster está configurado con un grupo de subredes personalizado. El control falla si CacheSubnetGroupName un ElasticCache clúster tiene el valor default.

Al lanzar un ElasticCache clúster, se crea un grupo de subredes predeterminado si aún no existe ninguno. El grupo predeterminado utiliza subredes de la nube privada virtual (VPC) predeterminada. Recomendamos usar grupos de subredes personalizados que restrinjan más las subredes en las que reside el clúster y las redes que el clúster hereda de las subredes.

Corrección

Para crear un nuevo grupo de subredes para un ElasticCache clúster, consulte [Creación de un grupo de subredes](#) en la Guía del ElasticCache usuario de Amazon.

Controles de Security Hub para Elastic Beanstalk

Estos AWS Security Hub controles evalúan el AWS Elastic Beanstalk servicio y los recursos.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[ElasticBeanstalk.1] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados

Requisitos relacionados: NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2

Categoría: Detectar > Servicios de detección > Supervisión de aplicaciones

Gravedad: baja

Tipo de recurso: AWS::ElasticBeanstalk::Environment

Regla de AWS Config : [beanstalk-enhanced-health-reporting-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los informes de estado mejorados están habilitados para sus entornos AWS Elastic Beanstalk .

Los informes de estado mejorados de Elastic Beanstalk permiten una respuesta más rápida a los cambios en el estado de la infraestructura subyacente. Estos cambios podrían provocar una falta de disponibilidad de la aplicación.

Los informes de estado mejorados de Elastic Beanstalk proporcionan un descriptor de estado para evaluar la gravedad de los problemas detectados e identificar las posibles causas que se deben investigar. El agente de estado de Elastic Beanstalk, incluido en Amazon Machine AMIs Images () compatible, evalúa los registros y las métricas de las instancias del entorno. EC2

Para obtener información adicional, consulte la [Supervisión y los informes de estado mejorados](#) en la Guía para desarrolladores de AWS Elastic Beanstalk .

Corrección

Para obtener instrucciones sobre cómo habilitar los informes de estado mejorados, consulte [Habilitar los informes de estado mejorados mediante la consola de Elastic Beanstalk](#) en la Guía para desarrolladores de AWS Elastic Beanstalk .

[ElasticBeanstalk.2] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas

Requisitos relacionados: NIST.800-53.r5 SI-2, niST.800-53.r5 SI-2 (2), niST.800-53.r5 SI-2 (4), Nist.800-53.r5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: alta

Tipo de recurso: AWS::ElasticBeanstalk::Environment

Regla de AWS Config : [elastic-beanstalk-managed-updates-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
UpdateLevel	Nivel de actualización de la versión	Enum	minor, patch	Sin valor predeterminado

Este control comprueba si las actualizaciones de la plataforma administradas están habilitadas para un entorno de Elastic Beanstalk. Se produce un error en el control si no están habilitadas las actualizaciones de la plataforma administradas. De manera predeterminada, el control pasa si algún tipo de actualización de la plataforma está habilitado. De manera opcional, puede proporcionar un valor personalizado de parámetro para requerir un nivel de actualización específico.

Al habilitar las actualizaciones de plataforma administradas, se garantiza que se instalen las últimas correcciones, actualizaciones y funciones de la plataforma disponibles para el entorno. Mantenerse al día con la instalación de los parches es un paso importante para proteger los sistemas.

Corrección

Para habilitar las actualizaciones de la plataforma administradas, consulte [Configuración de las actualizaciones de la plataforma administradas en la sección Actualizaciones de la plataforma administradas](#) de la Guía para desarrolladores de AWS Elastic Beanstalk .

[ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch

Requisitos relacionados: PCI DSS v4.0.1/10.4.2

Categoría: Identificar - Registro

Gravedad: alta

Tipo de recurso: AWS::ElasticBeanstalk::Environment

Regla de AWS Config : [elastic-beanstalk-logs-to-cloudwatch](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
RetentionInDays	Cantidad de días que se van a conservar los eventos de registro antes de que expiren	Enum	1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827, 3653	Sin valor predeterminado

Este control comprueba si un entorno de Elastic Beanstalk está configurado para enviar registros a Logs. CloudWatch El control falla si el entorno de Elastic Beanstalk no está configurado para enviar registros a Logs. CloudWatch De manera opcional, puede proporcionar un valor personalizado para el parámetro RetentionInDays si quiere que el control pase únicamente si los registros se retienen durante la cantidad de días especificada antes de que expiren.

CloudWatch le ayuda a recopilar y monitorear diversas métricas para sus aplicaciones y recursos de infraestructura. También se puede utilizar CloudWatch para configurar acciones de alarma en función de métricas específicas. Recomendamos integrar Elastic CloudWatch Beanstalk con para obtener una mayor visibilidad del entorno de Elastic Beanstalk. Los registros de Elastic Beanstalk incluyen el archivo eb-activity.log, los registros de acceso del entorno nginx o el servidor proxy Apache y los registros específicos de un entorno.

Corrección

Para integrar Elastic CloudWatch Beanstalk con Logs, [consulte Transmitir registros de instancias a Logs en la Guía para CloudWatch desarrolladores](#).AWS Elastic Beanstalk

Controles de Security Hub para equilibradores de carga elásticos

Estos AWS Security Hub controles de evalúan el servicio y los recursos del equilibrador de carga elástico. Es posible que los controles de no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[ELB.1] El equilibrador de carga de aplicación debe configurarse para redirigir todas las solicitudes HTTP a HTTPS

Requisitos relacionados: PCI DSS v3.2.1/2.3, PCI DSS v3.2.1/4.1, NIST.800-53.r5 AC-1 7 (2), (1), 2 NIST.800-53.r5 IA-5 (5) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 PCI DSS v3.r5 SI-7 (6), NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6) NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8

Categoría: Detectar - Servicios de detección

Gravedad: media

Tipo de recurso: AWS::ElasticLoadBalancingV2::LoadBalancer

Regla de AWS Config : [alb-http-to-https-redirect-check](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el redireccionamiento de HTTP a HTTPS está configurado en todos los oyentes HTTP de los equilibradores de carga de aplicación. El control falla si alguno de los detectores HTTP de los equilibradores de carga de aplicaciones no tiene configurada la redirección de HTTP a HTTPS.

Antes de comenzar a utilizar el equilibrador de carga de aplicación, debe agregar al menos uno o más oyentes. Un agente de escucha es un proceso que utiliza el protocolo y el puerto configurados para comprobar las solicitudes de conexión. Los oyentes admiten los protocolos HTTP y HTTPS. Puede utilizar un oyente HTTPS para descargar el trabajo de cifrado y descifrado a su equilibrador de carga. Para forzar el cifrado en tránsito, debe usar acciones de redireccionamiento con los equilibradores de carga de aplicación para redirigir las solicitudes HTTP del cliente hacia una solicitud HTTPS en el puerto 443.

Para obtener más información, consulte [Creación de un agente de escucha para el Equilibrador de carga de aplicación](#) en la Guía del usuario de Equilibrador de carga de aplicaciones.

Corrección

Para redirigir las solicitudes HTTP a HTTPS, debe agregar una regla de escucha de Equilibrador de carga de aplicación o editar una regla existente.

Para obtener instrucciones sobre cómo agregar una nueva regla, consulte [Agregar una regla](#) en la Guía del usuario de los equilibradores de carga de aplicaciones. En Protocolo : Puerto, elija HTTP y luego ingrese **80**. En Añadir acción, Redirigir a, elija HTTPS y, a continuación, introduzca **443**.

Para obtener instrucciones sobre cómo editar una regla existente, consulte [Editar una regla](#) en la Guía del usuario de los equilibradores de carga de aplicaciones. En Protocolo : Puerto, elija HTTP y luego ingrese **80**. En Añadir acción, Redirigir a, elija HTTPS y, a continuación, introduzca **443**.

[ELB.2] Los equilibradores de carga clásicos con agentes de escucha SSL/HTTPS deben usar un certificado proporcionado por AWS Certificate Manager

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, 2 NIST.800-53.r5 IA-5 (3), 3, 3 (5), NIST.800-53.r5 SC-1 (4), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-2 (NIST.800-53.r5 SC-12), NIST.800-53.r5 SC-7 NIST.800-53.r5 NIST.800-53.r5 SC-8 SI-7 NIST.800-53.r5 SC-8 (6), NIST.800-53.r5 SC-8 NIST.800-171.r2 3.13.8

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::ElasticLoadBalancing::LoadBalancer

Regla de AWS Config : [elb-acm-certificate-required](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Comprueba si los Equilibrador de carga clásicos utilizan los certificados SSL proporcionados por AWS Certificate Manager . El control falla si el Equilibrador de carga clásico configurado con el agente de escucha HTTPS/SSL no utiliza un certificado proporcionado por ACM.

Para crear un certificado, puede utilizar ACM o una herramienta que admita los protocolos SSL y TLS, como OpenSSL. Security Hub recomienda que utilice ACM para crear o importar certificados para su equilibrador de carga.

ACM se integra con Equilibrador de carga clásico, lo que le permite implementar el certificado en el equilibrador de carga. También debe renovar estos certificados automáticamente.

Corrección

Para obtener información sobre cómo asociar un certificado SSL/TLS de ACM a un Equilibrador de carga clásico, consulte el artículo del AWS Knowledge Center [¿Cómo puedo asociar un certificado SSL/TLS de ACM a un Classic, Application o Equilibrador de carga de red?](#)

[ELB.3] Los oyentes de Equilibrador de carga clásico deben configurarse con una terminación HTTPS o TLS

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), (1), 3, 3, 3 (3), (2), NIST.800-53.r5 IA-5 (NIST.800-53.r5 SC-12) NIST.800-53.r5 AC-4, NIST.800-171.r5 SI-7 (6), NIST.800-171.r2 3.13.8, NIST.800-53.r5 SC-1 NIST.800-171.r2 3.13.15, NIST.800-53.r5 SC-2 NIST.800-171.r2 3.13.15, NIST.800-53.r5 SC-2 NIST.800-171.r2 3.13.15, NIST.800-53.r5 SC-7 NIST.800-171.r2 3.13.15, NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-171.r2 3.13.15, NIST.800-53.r5 SC-8 NIST.800-171.r2 3.13.15, NIST.800-171.r2 3.13.15, NIST.800-171.r2 3.13.15, NIST.800-171.r2 3.13.15, NIST.800-171.r2 3.13.15, NIST.800-171.r5

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::ElasticLoadBalancing::LoadBalancer

Regla de AWS Config : [elb-tls-https-listeners-only](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los agentes de escucha de Equilibrador de carga clásico están configurados con el protocolo HTTPS o TLS para las conexiones frontend (entre el cliente y el equilibrador de carga). El control se aplica si un Equilibrador de carga clásico tiene oyentes. Si su Equilibrador de carga clásico no tiene un listener configurado, el control no informa de ningún resultado.

El control pasa si los oyentes de Equilibrador de carga clásico están configurados con TLS o HTTPS para las conexiones front-end.

El control falla si el listener no está configurado con TLS o HTTPS para las conexiones front-end.

Antes de comenzar a utilizar un equilibrador de carga, debe agregar uno o más oyentes. Un agente de escucha es un proceso que utiliza el protocolo y el puerto configurados para comprobar las solicitudes de conexión. Los oyentes pueden admitir los protocolos HTTP y HTTPS/TLS. Siempre debe usar un agente de escucha HTTPS o TLS para que el equilibrador de cargas se encargue de cifrar y descifrar en tránsito.

Corrección

Para solucionar este problema, actualiza tus oyentes para que usen el protocolo TLS o HTTPS.

Cómo cambiar todos los oyentes no compatibles por oyentes TLS/HTTPS

1. Abre la EC2 consola de Amazon en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, en Equilibración de carga, elija equilibradores de carga.
3. Etiquetado del equilibrador de carga clásico
4. En la pestaña Listeners (Agentes de escucha), seleccione Edit (Editar).
5. Para todos los oyentes en los que el Protocolo Equilibrador de carga no esté configurado en HTTPS o SSL, cambie la configuración a HTTPS o SSL.
6. Para todos los oyentes modificados, en la pestaña Certificados, seleccione Cambiar el valor predeterminado.
7. Para los certificados ACM e IAM, seleccione un certificado.
8. Seleccione Guardar como predeterminado.
9. Tras actualizar todos los oyentes, selecciona Guardar.

[ELB.4] El equilibrador de carga de aplicación debe configurarse para eliminar los encabezados http no válidos

Requisitos relacionados: NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0.1/6.2.4

Categoría: Proteger > Seguridad de red

Gravedad: media

Tipo de recurso: AWS::ElasticLoadBalancingV2::LoadBalancer

Regla de AWS Config : [alb-http-drop-invalid-header-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control evalúa si un equilibrador de carga de aplicación está configurado para eliminar los encabezados HTTP no válidos. El control falla si el valor `routing.http.drop_invalid_header_fields.enabled` se establece como `false`.

De forma predeterminada, los equilibradores de carga de aplicaciones no están configurados para eliminar valores de encabezado HTTP no válidos. La eliminación de estos valores de encabezado evita los ataques de desincronización de HTTP.

 Note

Recomendamos deshabilitar este control si ELB.12 está habilitado en su cuenta. Para obtener más información, consulte [\[ELB.12\] Equilibrador de carga de aplicación debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#).

Corrección

Para solucionar este problema, configura tu equilibrador de cargas para eliminar los campos de encabezado no válidos.

Cómo configurar el equilibrador de carga para eliminar campos de encabezado no válidos

1. Abre la EC2 consola de Amazon en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija Load balancers (Balanceadores de carga).
3. Eliminación de un Equilibrador de carga de aplicación
4. Para Acciones, elija Editar atributos.
5. En Eliminar campos de encabezado no válidos, selecciona Activar.
6. Seleccione Save.

[ELB.5] El registro de las aplicaciones y de los equilibradores de carga clásicos debe estar habilitado

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::ElasticLoadBalancing::LoadBalancer,
AWS::ElasticLoadBalancingV2::LoadBalancer

Regla de AWS Config : [elb-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el Equilibrador de carga de aplicación y el Equilibrador de carga clásico tienen el registro activado. El control tiene errores si `access_logs.s3.enabled` es `false`.

Elastic Load Balancing proporciona registros de acceso que capturan información detallada sobre las solicitudes enviadas al equilibrador de carga. Cada registro contiene distintos datos, como el momento en que se recibió la solicitud, la dirección IP del cliente, las latencias, las rutas de solicitud y las respuestas del servidor. Puede utilizar estos registros de acceso para analizar los patrones de tráfico y solucionar problemas.

Para obtener más información, consulte [Etiquetado del Equilibrador de carga clásico](#) en la Guía del usuario de Equilibrador de carga clásicos.

Corrección

Para habilitar los registros de acceso, consulte el [Paso 3: Configurar los registros de acceso](#) en la Guía del usuario de los equilibradores de carga de aplicaciones.

[ELB.6] La protección contra la eliminación de un equilibrador de carga de aplicación, de puerta de enlace y de red debe estar habilitada

Requisitos relacionados: (1), (2) NIST.800-53.r5 CA-9 NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::ElasticLoadBalancingV2::LoadBalancer

Regla de AWS Config : [elb-deletion-protection-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el equilibrador de carga de red, de puerta de enlace o de aplicación tiene habilitada la protección contra eliminación. El control falla si la protección contra la eliminación está deshabilitada.

Habilite la protección contra eliminación para evitar que el equilibrador de carga de red, de puerta de enlace o de aplicación se elimine.

Corrección

Para evitar que el equilibrador de carga se elimine por error, puede habilitar la protección contra eliminación. De forma predeterminada, la protección contra eliminación del equilibrador de carga está deshabilitada.

Si habilita la protección contra eliminación del equilibrador de carga, deberá deshabilitarla para poder eliminarlo.

Para habilitar la protección contra la eliminación de un equilibrador de carga de aplicación, consulte la sección [Protección contra la eliminación](#) en la Guía del usuario de los equilibradores de carga de aplicaciones. Para habilitar la protección contra la eliminación de un equilibrador de carga de puerta de enlace, consulte la sección [Protección contra la eliminación](#) en la Guía del usuario de los equilibradores de carga de puerta de enlace. Para habilitar la protección contra la eliminación de un equilibrador de carga de red, consulte la sección [Protección contra la eliminación](#) en la Guía del usuario de los equilibradores de carga de red.

[ELB.7] Los equilibradores de carga clásicos deberían tener habilitado el drenaje de conexiones

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Recuperación > Resiliencia

Gravedad: media

Tipo de recurso: AWS::ElasticLoadBalancing::LoadBalancer

Regla de AWS Config: elb-connection-draining-enabled (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los equilibradores de carga clásicos tienen habilitado el drenaje de conexión.

Al habilitar el drenaje de conexiones en los Equilibradores de carga clásicos se garantiza que el equilibrador de carga deje de enviar solicitudes a instancias que están en proceso de anulación del registro o se encuentran en mal estado. Mantiene abiertas las conexiones existentes. Esto es particularmente útil para instancias en grupos de escalado automático, para garantizar que las conexiones no se interrumpan abruptamente.

Corrección

Para habilitar el drenaje de conexión en Equilibrador de carga clásico, consulte [Configuración del drenaje de conexión para el Equilibrador de carga clásico](#) en la Guía del usuario de Equilibrador de carga clásico.

[ELB.8] Los equilibradores de carga clásicos con agentes de escucha SSL deben usar una política de seguridad predefinida que tenga una duración sólida AWS Config

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), (1), 3, 3, 3 (3), (2), NIST.800-53.r5 IA-5 (NIST.800-53.r5 SC-12) NIST.800-53.r5 AC-4, NIST.800-171.r5 SI-7 (6), NIST.800-171.r2 3.13.8, NIST.800-53.r5 SC-1 NIST.800-171.r2 3.13.15, NIST.800-53.r5 SC-2 NIST.800-171.r2 3.13.15, NIST.800-53.r5 SC-2 NIST.800-171.r2 3.13.15, NIST.800-53.r5 SC-7 NIST.800-171.r2 3.13.15 NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-171.r2 3.13.15, NIST.800-53.r5 SC-8 NIST.800-171.r2 3.13.15, NIST.800-171.r2 3.13.15, NIST.800-171.r2 3.13.15, NIST.800-171.r2 3.13.15, NIST.800-171.r5

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::ElasticLoadBalancing::LoadBalancer

Regla de AWS Config : [elb-predefined-security-policy-ssl-check](#)

Tipo de horario: provocado por un cambio

Parámetros:

- predefinedPolicyName: ELBSecurityPolicy-TLS-1-2-2017-01 (no personalizable)

Este control comprueba si los oyentes HTTPS/SSL de Equilibrador de carga clásico utilizan la política predefinida de `ELBSecurityPolicy-TLS-1-2-2017-01`. El control falla si los oyentes HTTPS/SSL de Equilibrador de carga clásico no utilizan `ELBSecurityPolicy-TLS-1-2-2017-01`.

Una política de seguridad es una combinación de protocolos SSL, cifrados y la opción de preferencia del orden del servidor. Las políticas predefinidas controlan los cifrados, los protocolos y los órdenes de preferencia que se deben admitir durante las negociaciones SSL entre un cliente y un equilibrador de carga.

Usar `ELBSecurityPolicy-TLS-1-2-2017-01` puede ayudarlo a cumplir con los estándares de cumplimiento y seguridad que requieren que deshabilite versiones específicas de SSL y TLS. Para obtener más información, consulte [Agentes de escucha para el Equilibrador de carga clásico](#) en la Guía del usuario de Equilibrador de carga clásicos.

Corrección

Para obtener información sobre cómo utilizar la política de seguridad predefinida de `ELBSecurityPolicy-TLS-1-2-2017-01` con un Equilibrador de carga clásico, consulte [Configurar los ajustes de seguridad](#) en la Guía del usuario de Equilibrador de carga clásicos.

[ELB.9] Los equilibradores de carga clásicos deberían tener habilitado el equilibrio de carga entre zonas

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancing::LoadBalancer`

Regla de AWS Config : [elb-cross-zone-load-balancing-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el equilibrio de carga entre zonas está habilitado para los equilibradores de carga clásicos (CLBs). El control falla si el equilibrio de carga entre zonas no está habilitado para un CLB.

Cada nodo del equilibrador de carga distribuye el tráfico entre los destinos registrados en su zona de disponibilidad solamente. Cuando el equilibrio de carga entre zonas está deshabilitado, cada nodo del equilibrador de carga distribuye el tráfico únicamente entre los destinos registrados de su zona de disponibilidad. Si el número de destinos registrados no es el mismo en todas las zonas de disponibilidad, el tráfico no se distribuirá de manera uniforme y las instancias de una zona podrían terminar sobreutilizadas en comparación con las instancias de otra zona. Con cross-zone load balancing, cada nodo del equilibrador de carga de su equilibrador de carga clásico distribuye las solicitudes equitativamente entre todas las instancias registradas en todas las zonas de disponibilidad habilitadas. Para obtener más información, [consulte Equilibrio de carga entre zonas](#) en la Guía del usuario de Elastic Load Balancing.

Corrección

Para habilitar el balanceo de cargas entre zonas en un Equilibrador de carga clásico, consulta [Habilitar el balanceo de cargas entre zonas](#) en la Guía del usuario de Equilibrador de carga clásicos.

[ELB.10] Equilibrador de carga clásico debe abarcar varias zonas de disponibilidad

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::ElasticLoadBalancing::LoadBalancer

Regla de AWS Config : [clb-multiple-az](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
minAvailabilityZones	Cantidad mínima de zonas de disponibilidad	Enum	2, 3, 4, 5, 6	2

Este control comprueba si se configuró un Classic Load Balancer para abarcar al menos la cantidad especificada de zonas de disponibilidad (AZs). Se produce un error en el control si el Classic Load Balancer no abarca al menos la cantidad especificada de AZs. A menos que se proporcione un valor personalizado de parámetro para la cantidad mínima de AZs, Security Hub utiliza un valor predeterminado de dos AZs.

Puede configurar el Classic Load Balancer para que las solicitudes de entrada se distribuyan entre las EC2 instancias de Amazon de una única zona de disponibilidad o de varias. Un Equilibrador de carga clásico que no abarque varias zonas de disponibilidad no puede redirigir el tráfico a destinos de otra zona de disponibilidad si la única zona de disponibilidad configurada deja de estar disponible.

Corrección

Para agregar zonas de disponibilidad a un equilibrador de carga clásico, consulte [Add or remove subnets for your Classic Load Balancer](#) en la Guía del usuario para los Equilibradores de carga clásicos.

[ELB.12] Equilibrador de carga de aplicación debe configurarse con el modo defensivo o de mitigación de desincronización más estricto

Requisitos relacionados: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, PCI DSS v4.0.1/6.2.4

Categoría: Protección > Protección de datos > Integridad de los datos

Gravedad: media

Tipo de recurso: AWS::ElasticLoadBalancingV2::LoadBalancer

Regla de AWS Config : [alb-desync-mode-check](#)

Tipo de horario: provocado por un cambio

Parámetros:

- desyncMode: defensive, strictest (no personalizable)

Este control comprueba si un Equilibrador de carga de aplicación está configurado con el modo defensivo o con el modo de mitigación de desincronización más estricto. El control falla si un Equilibrador de carga de aplicación no está configurado con el modo defensivo o de mitigación de desincronización más estricto.

Los problemas de desincronización de HTTP pueden provocar el contrabando de solicitudes y hacer que las aplicaciones sean vulnerables al envenenamiento de las colas de solicitudes o de la caché. A su vez, estas vulnerabilidades pueden provocar el uso indebido de credenciales o la ejecución de comandos no autorizados. Los equilibradores de carga de aplicaciones configurados con el modo defensivo o el modo de mitigación de desincronización más estricto protegen tu aplicación de los problemas de seguridad que pueda provocar la desincronización de HTTP.

Corrección

Para actualizar el modo de mitigación de desincronización de un Equilibrador de carga de aplicación, [consulte el modo de mitigación de desincronización](#) en la Guía del usuario de Equilibrador de carga de aplicaciones.

[ELB.13] Los equilibradores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::ElasticLoadBalancingV2::LoadBalancer

Regla de AWS Config : [elbv2-multiple-az](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
minAvailabilityZones	Cantidad mínima de zonas de disponibilidad	Enum	2, 3, 4, 5, 6	2

Este control comprueba si un Elastic Load Balancer V2 (equilibrador de carga de aplicaciones, redes o puertas de enlace) registró instancias de al menos la cantidad especificada de zonas de disponibilidad (). AZs Se produce un error en el control si un Elastic Load Balancer V2 no tiene instancias registradas en al menos la cantidad especificada de. AZs A menos que se proporcione un valor personalizado de parámetro para la cantidad mínima de AZs, Security Hub utiliza un valor predeterminado de dos AZs.

Elastic Load Balancing distribuye automáticamente el tráfico entrante entre varios destinos, por ejemplo, EC2 instancias, contenedores y direcciones IP en una o varias zonas de disponibilidad. Elastic Load Balancing escala el equilibrador de carga a medida que el tráfico entrante va cambiando con el tiempo. Se recomienda configurar al menos dos zonas de disponibilidad para garantizar la disponibilidad de los servicios, ya que el Elastic Load Balancer podrá dirigir el tráfico a otra zona de disponibilidad si alguna deja de estar disponible. Tener configuradas varias zonas de disponibilidad ayudará a evitar que la aplicación tenga un único punto de error.

Corrección

Para agregar una zona de disponibilidad a un Equilibrador de carga de aplicación, consulte [Zonas de disponibilidad para el equilibrador de carga de aplicaciones](#) en la Guía del usuario para equilibradores de carga de aplicaciones. Para crear un equilibrador de carga de red, consulte [Introducción a los equilibradores de carga de red](#) en la Guía del usuario de los equilibradores de carga de red. Para añadir una zona de disponibilidad a un equilibrador de carga de puerta de enlace, consulte [Crear un equilibrador de carga de puerta de enlace](#) en la Guía del usuario de equilibradores de carga de puerta de enlace.

[ELB.14] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto

Requisitos relacionados: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, PCI DSS v4.0.1/6.2.4

Categoría: Protección > Protección de datos > Integridad de los datos

Gravedad: media

Tipo de recurso: AWS::ElasticLoadBalancing::LoadBalancer

Regla de AWS Config : [clb-desync-mode-check](#)

Tipo de horario: provocado por un cambio

Parámetros:

- `desyncMode`: `defensive`, `strictest` (no personalizable)

Este control comprueba si un Equilibrador de carga clásico está configurado con el modo defensivo o con el modo de mitigación de desincronización más estricto. El control falla si el Equilibrador de carga clásico no está configurado con el modo defensivo o de mitigación de desincronización más estricto.

Los problemas de desincronización de HTTP pueden provocar el contrabando de solicitudes y hacer que las aplicaciones sean vulnerables al envenenamiento de las colas de solicitudes o de la caché. A su vez, estas vulnerabilidades pueden provocar el secuestro de credenciales o la ejecución de comandos no autorizados. Los equilibradores de carga clásicos configurados con el modo defensivo o el modo de mitigación de desincronización más estricto protegen tu aplicación de los problemas de seguridad que pueda provocar la desincronización de HTTP.

Corrección

Para actualizar el modo de mitigación de desincronización en un Equilibrador de carga clásico, consulte [Modificar el modo de mitigación de desincronización](#) en la Guía del usuario de Equilibrador de carga clásico.

[ELB.16] Los equilibradores de carga de aplicaciones deben estar asociados a una ACL web de AWS WAF

Requisitos relacionados: NIST.800-53.r5 AC-4 (21)

Categoría: Proteger > Servicios de protección

Gravedad: media

Tipo de recurso: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regla de AWS Config : [alb-waf-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un Application Load Balancer está asociado a una lista de control de acceso AWS WAF web (ACL web) AWS WAF clásico o. El control falla si el campo `Enabled` de la configuración AWS WAF se ha establecido como `false`.

AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones web APIs de ataques. Con AWS WAF puede configurar una web ACL, que son un conjunto de reglas que permiten, bloquean o cuentan solicitudes web en función de las reglas y condiciones de seguridad web personalizables que defina. Recomendamos asociar el Equilibrador de carga de aplicación a una ACL web de AWS WAF para protegerlo de ataques malintencionados.

Corrección

Para asociar un Application Load Balancer a una ACL web, consulte [Asociar o desasociar una ACL web con AWS recurso de en la Guía para desarrolladores](#) de AWS WAF

[ELB.17] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3 (3), NIST.800-53.r5 SC-1 (4), NIST.800-53.r5 SC-2 (4), (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6) NIST.800-53.r5 SC-2

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::ElasticLoadBalancingV2::Listener

Regla de AWS Config : [elbv2-predefined-security-policy-ssl-check](#)

Tipo de horario: provocado por un cambio

Parámetros **sslPolicies**: ELBSecurityPolicy-TLS13-1-2-2021-06, ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04, ELBSecurityPolicy-TLS13-1-3-2021-06, ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04, ELBSecurityPolicy-TLS13-1-2-Res-2021-06, ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 (no personalizables)

Este control comprueba si el agente de escucha HTTPS de un Application Load Balancer o el agente de escucha TLS de un Network Load Balancer están configurados para cifrar los datos en tránsito mediante una política de seguridad recomendada. Se produce un error en el control si el agente de escucha HTTPS o TLS de un equilibrador de carga no está configurado para usar una política de seguridad recomendada.

Elastic Load Balancing utiliza una configuración de negociación SSL, conocida como política de seguridad, para negociar las conexiones entre un cliente y un equilibrador de carga. La política de seguridad especifica una combinación de protocolos y cifrados. El protocolo establece una conexión segura entre un cliente y un servidor. Un cifrado es un algoritmo de cifrado que usa claves de cifrado para crear un mensaje codificado. Durante el proceso de negociación de conexiones, el cliente y el equilibrador de carga presentan una lista con los cifrados y protocolos que admite cada uno por orden de preferencia. El uso de una política de seguridad recomendada para un balanceador de carga puede ayudarte a cumplir con los estándares de seguridad y cumplimiento.

Corrección

Para obtener información sobre las políticas de seguridad recomendadas y cómo actualizar los listeners, consulte las siguientes secciones de las guías del usuario de Elastic Load Balancing: [Políticas de seguridad para los balanceadores de carga de aplicaciones](#), [Políticas de seguridad para los balanceadores de carga de red](#), [Actualizar un listener HTTPS para su Application Load Balancer](#) y [Actualizar un listener para su Network Load Balancer](#).

Security Hub para Elasticsearch

Estos AWS Security Hub controles evalúan el servicio y los recursos de Elasticsearch.

Es posible que estos controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[ES.1] Los dominios de Elasticsearch deben tener habilitado el cifrado en reposo

Requisitos relacionados: PCI DSS v3.2.1/3.4, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SC-2 Nist.800-53.r5 NIST.800-53.r5 SC-7 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::Elasticsearch::Domain

Regla de AWS Config : [elasticsearch-encrypted-at-rest](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si los dominios de Elasticsearch tienen habilitada la configuración de cifrado en reposo. La comprobación falla si el cifrado en reposo no está habilitado.

Para aumentar la seguridad de sus datos confidenciales OpenSearch, debe configurarlos OpenSearch para que estén cifrados en reposo. Los dominios Elasticsearch ofrecen cifrado de datos en reposo. La función se utiliza AWS KMS para almacenar y administrar sus claves de cifrado. Para realizar el cifrado, utiliza el algoritmo Estándar de cifrado avanzado con claves de 256 bits (AES-256).

Para obtener más información sobre el OpenSearch cifrado en reposo, consulta [Cifrado de datos en reposo para Amazon OpenSearch Service](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

Algunos tipos de instancias, como `t.small` y `t.medium`, no admiten el cifrado de datos en reposo. Para obtener más información, consulta los [tipos de instancias compatibles](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

Corrección

Para habilitar el cifrado en reposo para dominios de Elasticsearch nuevos y existentes, consulta [Habilitar el cifrado de datos en reposo en](#) la Guía para desarrolladores de Amazon OpenSearch Service.

[ES.2] Los dominios de Elasticsearch no deben ser de acceso público

Requisitos relacionados: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7), (21), NIST.800-53.r5 AC-3, (11) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (16), (20) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7

Categoría: Proteger > Configuración de red segura > Recursos dentro de VPC

Gravedad: crítica

Tipo de recurso: AWS::Elasticsearch::Domain

Regla de AWS Config : [elasticsearch-in-vpc-only](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si los dominios de Elasticsearch están en una VPC. No evalúa la configuración de direccionamiento de subred de VPC para determinar el acceso público. Debe asegurarse de que los dominios de Elasticsearch no están asociados a subredes públicas. Consulta [las políticas basadas en recursos](#) en la Guía para desarrolladores de Amazon OpenSearch Service. También debe asegurarse de que la VPC esté configurada de acuerdo con las prácticas recomendadas. Consulte [Prácticas recomendadas de seguridad para su VPC](#) en la Guía del usuario de Amazon VPC.

Los dominios de Elasticsearch implementados en una VPC pueden comunicarse con los recursos de la VPC a través de la AWS red privada, sin necesidad de atravesar la Internet pública. Esta configuración aumenta la seguridad al limitar el acceso a los datos en tránsito. VPCs proporcionan una serie de controles de red para proteger el acceso a los dominios de Elasticsearch, incluidas las ACL de red y los grupos de seguridad. Security Hub recomienda migrar los dominios públicos de Elasticsearch VPCs para aprovechar estos controles.

Corrección

Si crea un dominio con un punto de enlace público, no podrá colocarlo posteriormente en una VPC. En lugar de ello, se debe crear un dominio nuevo y migrar los datos. y viceversa. Si crea un dominio dentro de una VPC, no puede tener un punto de enlace público. En su lugar, debe [crear otro dominio](#) o deshabilitar este control.

Consulte Cómo [lanzar sus dominios de Amazon OpenSearch Service dentro de una VPC](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

[ES.3] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos

Requisitos relacionados: NIST.800-53.r5 SC-1 3 NIST.800-53.r5 AC-4, 3 (NIST.800-53.r5 SC-23), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-7 (1), NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2) NIST.800-53.r5 SC-8, PCI DSS v4.0.1/4.2.1

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::Elasticsearch::Domain

Regla de AWS Config : [elasticsearch-node-to-node-encryption-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un dominio de Elasticsearch tiene el node-to-node cifrado activado. El control falla si el dominio de Elasticsearch no tiene el cifrado activado. node-to-node El control también produce resultados erróneos si una versión de Elasticsearch no admite las comprobaciones de cifrado. node-to-node

El protocolo HTTPS (TLS) se puede utilizar para evitar que posibles atacantes escuchen o manipulen el tráfico de la red mediante ataques u otros similares. person-in-the-middle Solo se deben permitir las conexiones cifradas a través de HTTPS (TLS). Al habilitar el node-to-node cifrado en los dominios de Elasticsearch, se garantiza que las comunicaciones dentro del clúster se cifren durante el tránsito.

Puede haber una penalización en el rendimiento asociada a esta configuración. Debe conocer y probar la compensación de rendimiento antes de activar esta opción.

Corrección

Para obtener información sobre cómo habilitar el node-to-node cifrado en dominios nuevos y existentes, consulta [Habilitar el node-to-node cifrado](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

[ES.4] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), Nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.r5 SI-4 (20), Nist.800-53.r5 SI-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::Elasticsearch::Domain

Regla de AWS Config : [elasticsearch-logs-to-cloudwatch](#)

Tipo de horario: provocado por un cambio

Parámetros:

- `logtype = 'error'` (no personalizable)

Este control comprueba si los dominios CloudWatch de Elasticsearch están configurados para enviar registros de errores a Logs.

Debes habilitar los registros de errores para los dominios de Elasticsearch y enviar esos CloudWatch registros a Logs para su retención y respuesta. Los registros de errores de los dominios pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

Corrección

Para obtener información sobre cómo habilitar la publicación de registros, consulte [Habilitar la publicación de registros \(consola\)](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

[ES.5] Los dominios de Elasticsearch deben tener habilitado el registro de auditoría

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.4.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::Elasticsearch::Domain`

Regla de AWS Config : `elasticsearch-audit-logging-enabled` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

- `cloudWatchLogsLogGroupArnList` (no personalizable). Security Hub no rellena este parámetro. Lista CloudWatch de grupos de registros separados por comas que deben configurarse para los registros de auditoría.

Esta regla se aplica NON_COMPLIANT si el grupo de CloudWatch registros de registros del dominio de Elasticsearch no está especificado en esta lista de parámetros.

Este control comprueba si los dominios de Elasticsearch tienen habilitado el registro de auditoría. Este control falla si un dominio de Elasticsearch no tiene habilitado el registro de auditoría.

Los registros de auditoría son altamente personalizables. Te permiten realizar un seguimiento de la actividad de los usuarios en tus clústeres de Elasticsearch, incluidos los éxitos y los errores de autenticación, las solicitudes, los cambios de indexación y las consultas de búsqueda entrantes. OpenSearch

Corrección

Para obtener instrucciones detalladas sobre cómo habilitar los registros de auditoría, consulta [Habilitar los registros de auditoría](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

[ES.6] Los dominios de Elasticsearch deben tener al menos tres nodos de datos

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::Elasticsearch::Domain

Regla de AWS Config : elasticsearch-data-node-fault-tolerance (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los dominios de Elasticsearch están configurados con al menos tres nodos de datos y zoneAwarenessEnabled es true.

Un dominio de Elasticsearch requiere al menos tres nodos de datos para una alta disponibilidad y tolerancia a errores. La implementación de un dominio de Elasticsearch con al menos tres nodos de datos garantiza las operaciones del clúster en caso de que un nodo falle.

Corrección

Cómo modificar la cantidad de nodos de datos en un dominio de Elasticsearch

1. Abre la consola OpenSearch de Amazon Service en <https://console.aws.amazon.com/aos/>.
2. En Dominios, elija el nombre del dominio que desea editar.
3. Elija Edit domain (Editar dominio).
4. En Nodos de datos, estableza Número de nodos en un número mayor o igual a 3.

Para tres implementaciones de zonas de disponibilidad, establézcalo en un múltiplo de tres para garantizar una distribución equitativa entre las zonas de disponibilidad.

5. Elija Enviar.

[ES.7] Los dominios de Elasticsearch deben configurarse con al menos tres nodos maestros dedicados

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::Elasticsearch::Domain

Regla de AWS Config: elasticsearch-primary-node-fault-tolerance (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los dominios de Elasticsearch están configurados con al menos tres nodos principales dedicados. Este control falla si el dominio no utiliza nodos principales dedicados. Este control pasa si los dominios de Elasticsearch tienen cinco nodos principales dedicados. Sin embargo, el uso de más de tres nodos principales puede ser innecesario para mitigar el riesgo de disponibilidad y generará un costo adicional.

Un dominio de Elasticsearch requiere al menos tres nodos principales dedicados para una alta disponibilidad y tolerancia a los errores. Los recursos del nodo principal dedicado pueden agotarse

durante las implementaciones de los nodos de datos porque hay nodos blue/green adicionales que administrar. La implementación de un dominio de Elasticsearch con al menos tres nodos principales dedicados garantiza una capacidad suficiente de recursos del nodo principal y operaciones de clúster en caso de que un nodo falle.

Corrección

Para modificar la cantidad de nodos principales dedicados en un dominio OpenSearch

1. Abre la consola OpenSearch de Amazon Service en <https://console.aws.amazon.com/aos/>.
2. En Dominios, elija el nombre del dominio que desea editar.
3. Elija Edit domain (Editar dominio).
4. En Nodos maestros dedicados, defina el tipo de instancia en el tipo de instancia deseado.
5. Establezca el Número de nodos maestros en tres o más.
6. Elija Enviar.

[ES.8] Las conexiones a dominios de Elasticsearch deben estar cifradas conforme a la política de seguridad TLS más reciente

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3 (NIST.800-53.r5 SC-13), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), PCI DSS v4.0.1/4.2.1

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::Elasticsearch::Domain

Regla de AWS Config : elasticsearch-https-required (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un punto de conexión del dominio de Elasticsearch está configurado para utilizar la política de seguridad TLS más reciente. El control falla si el punto final del dominio de Elasticsearch no está configurado para usar la última política compatible o si HTTPS no está

habilitado. La política de seguridad TLS compatible más reciente es Policy-Min-TLS-1-2-PFS-2023-10.

Se puede usar HTTPS (TLS) para evitar que posibles atacantes utilicen ataques similares para espiar person-in-the-middle o manipular el tráfico de la red. Solo se deben permitir las conexiones cifradas a través de HTTPS (TLS). El cifrado de los datos en tránsito puede afectar al rendimiento. Debe probar su aplicación con esta característica para comprender el perfil de rendimiento y el impacto del TLS. TLS 1.2 proporciona varias mejoras de seguridad con respecto a las versiones anteriores de TLS.

Corrección

Para habilitar el cifrado TLS, utilice la operación de la API [UpdateDomainConfig](#) para configurar el objeto [DomainEndpointOptions](#). Esto establece la TLSecurityPolicy.

[ES.9] Los dominios de Elasticsearch deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Elasticsearch::Domain

Regla de AWS Config : tagged-elasticsearch-domain (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un dominio de Elasticsearch tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el dominio no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el dominio no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un dominio de Elasticsearch, consulta Cómo [trabajar con etiquetas](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

Controles de Security Hub en Amazon EMR

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon EMR (anteriormente denominado Amazon Elastic MapReduce). Es posible que los controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[EMR.1] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas

Requisitos relacionados: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7), (21), (11), (16), (20), (21), (3) NIST.800-53.r5 AC-3, (4) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (9) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: AWS::EMR::Cluster

AWS Config regla: emr-master-no-public [-ip](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si los nodos maestros de los clústeres de Amazon EMR tienen direcciones IP públicas. El control falla si hay direcciones IP públicas asociadas a alguna de las instancias del nodo maestro.

Las direcciones IP públicas se designan en el campo `PublicIp` de la configuración de `NetworkInterfaces` de la instancia. Este control solo comprueba los clústeres de Amazon EMR que se encuentran en un estado `RUNNING` o `WAITING`.

Corrección

Durante el lanzamiento, puedes controlar si a la instancia de una subred determinada o no determinada se le asigna una dirección pública. IPv4 De forma determinada, las subredes determinadas tienen este atributo configurado como `true`. Las subredes no determinadas tienen el atributo de direccionamiento IPv4 público establecido en `false`, a menos que lo haya creado el asistente de EC2 lanzamiento de instancias de Amazon. En ese caso, el atributo se establece como `true`.

Tras el lanzamiento, no puedes desasociar manualmente una IPv4 dirección pública de tu instancia.

Para corregir un error en la búsqueda, debe lanzar un nuevo clúster en una VPC con una subred privada que tenga IPv4 el atributo de direccionamiento público establecido en `false`. Para obtener instrucciones, consulte [Lanzamiento de clústeres en una VPC](#) en la Guía de administración de Amazon EMR.

[EMR.2] La configuración de bloqueo del acceso público de Amazon EMR debe estar habilitada

Requisitos relacionados: PCI DSS v4.0.1/1.4.4, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3,, (21), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6, (16) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoría: Proteger > Gestión del acceso seguro > Recurso no accesible públicamente

Gravedad: crítica

Tipo de recurso: AWS:::Account

Regla de AWS Config : [emr-block-public-access](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si su cuenta está configurada con el bloqueo de acceso público de Amazon EMR. Se produce un error en el control si la configuración de bloqueo de acceso público no está habilitada o si se permite cualquier puerto que no sea el 22.

El bloqueo de acceso público de Amazon EMR evita que lance un clúster en una subred pública si el clúster tiene una configuración de seguridad que permite el tráfico entrante desde direcciones IP públicas en un puerto. Cuando un usuario de su Cuenta de AWS lanza un clúster, Amazon EMR comprueba las reglas de puerto del grupo de seguridad del clúster y las compara con las reglas de tráfico entrante. Si el grupo de seguridad tiene una regla de entrada que abre los puertos a las direcciones IP públicas IPv4 0.0.0.0/0 o IPv6 :::/0, y esos puertos no se especifican como excepciones para su cuenta, Amazon EMR no permite que el usuario cree el clúster.

 Note

Bloquear el acceso público está habilitado de forma predeterminada. Si desea aumentar la protección de la cuenta, le recomendamos que lo mantenga habilitado.

Corrección

Para configurar el bloqueo de acceso público para Amazon EMR, consulte [Uso de Bloquear el acceso público de Amazon EMR](#) en la Guía de administración de Amazon EMR.

[EMR.3] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CP-9 (8), NIST.800-53.r5 SI-12

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::EMR::SecurityConfiguration

Regla de AWS Config : [emr-security-configuration-encryption-rest](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una configuración de seguridad de Amazon EMR tiene activado el cifrado en reposo. El control falla si la configuración de seguridad no habilita el cifrado en reposo.

Los datos en reposo hacen referencia a los datos que se almacenan en un almacenamiento persistente y no volátil durante cualquier periodo de tiempo. El cifrado de datos en reposo permite proteger la confidencialidad de los datos, lo que reduce el riesgo de que un usuario no autorizado pueda acceder a ellos.

Corrección

Para habilitar el cifrado en reposo en una configuración de seguridad de Amazon EMR, consulte [Configurar el cifrado de datos](#) en la Guía de administración de Amazon EMR.

[EMR.4] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito

Requisitos relacionados: NIST.800-53.r5 AC-4 NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-1 3, 3, NIST.800-53.r5 SC-2 3 (NIST.800-53.r5 SC-23)

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::EMR::SecurityConfiguration

Regla de AWS Config : [emr-security-configuration-encryption-transit](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una configuración de seguridad de Amazon EMR tiene activado el cifrado en tránsito. El control falla si la configuración de seguridad no habilita el cifrado en tránsito.

Los datos en tránsito hacen referencia a los datos que se mueven de una ubicación a otra, por ejemplo, entre los nodos del clúster o entre el clúster y la aplicación. Los datos pueden moverse a través de Internet o dentro de una red privada. El cifrado de los datos en tránsito reduce el riesgo de que un usuario no autorizado pueda espiar el tráfico de la red.

Corrección

Para habilitar el cifrado en tránsito en una configuración de seguridad de Amazon EMR, consulte [Configurar el cifrado de datos](#) en la Guía de administración de Amazon EMR.

Controles de Security Hub para EventBridge

Estos AWS Security Hub controles evalúan el EventBridge servicio y los recursos de Amazon.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[EventBridge.2] los autobuses de EventBridge eventos deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Events::EventBus`

AWS Config regla: `tagged-events-eventbus` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un bus de EventBridge eventos de Amazon tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el bus de eventos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el bus de eventos no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un autobús de EventBridge eventos, consulta las [EventBridge etiquetas de Amazon](#) en la Guía del EventBridge usuario de Amazon.

[EventBridge.3] Los autobuses de eventos EventBridge personalizados deben incluir una política basada en los recursos

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-2, (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 (3) NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, PCI DSS v4.0.1/10.3.1

Categoría: Proteger > Gestión del acceso seguro > Recurso no accesible públicamente

Gravedad: baja

Tipo de recurso: AWS::Events::EventBus

Regla de AWS Config : [custom-eventbus-policy-attached](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un bus de eventos EventBridge personalizado de Amazon tiene adjunta una política basada en recursos. Este control falla si el bus de eventos personalizado no tiene una política basada en recursos.

De forma predeterminada, un bus de eventos EventBridge personalizado no incluye una política basada en recursos. Esto permite a los directores de la cuenta acceder al bus de eventos. Al adjuntar

una política basada en recursos al bus de eventos, puede limitar el acceso al bus de eventos a cuentas específicas, así como conceder acceso intencionadamente a entidades de otra cuenta.

Corrección

Para adjuntar una política basada en recursos a un bus de eventos EventBridge personalizado, consulta [Uso de políticas basadas en recursos para Amazon en EventBridge](#) la Guía del usuario de Amazon. EventBridge

[EventBridge.4] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::Events::Endpoint

Regla de AWS Config : [global-endpoint-event-replication-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la replicación de eventos está habilitada para un punto final EventBridge global de Amazon. El control falla si la replicación de eventos no está habilitada para un punto de conexión global.

Los puntos finales globales ayudan a que su aplicación sea tolerante a los errores Regionales. Para empezar, debe asignar una comprobación de estado de Amazon Route 53 al punto de conexión. Cuando se inicia la conmutación por error, la comprobación de estado indica un estado “en mal estado”. A los pocos minutos del inicio de la conmutación por error, todos los eventos personalizados se enrutan a un bus de eventos en la región secundaria y son procesados por ese bus de eventos. Al utilizar puntos finales globales, puede habilitar la replicación de eventos. La replicación de eventos envía todos los eventos personalizados a los buses de eventos de las regiones principal y secundaria mediante reglas administradas. Recomendamos habilitar la replicación de eventos al configurar los puntos finales globales. La replicación de eventos le ayuda a comprobar que los puntos finales globales están configurados correctamente. La replicación de eventos es necesaria

para recuperarse automáticamente de un evento de conmutación por error. Si no tiene habilitada la replicación de eventos, tendrá que restablecer manualmente la comprobación de estado de Route 53 a “en buen estado” antes de que los eventos se redirijan a la región principal.

Note

Si utilizas autobuses de eventos personalizados, necesitarás un autobús de eventos personalizado en cada región con el mismo nombre y en la misma cuenta para que la conmutación por error funcione correctamente. Habilitación de la replicación de eventos puede aumentar su costo mensual. Para obtener información sobre los precios, consulta los [EventBridge precios de Amazon](#).

Corrección

Para habilitar la replicación de eventos para puntos de enlace EventBridge globales, consulte [Crear un punto de enlace global](#) en la Guía del EventBridge usuario de Amazon. Para la Replicación de eventos, seleccione Replicación de eventos habilitada.

Controles de Security Hub para Amazon Fraud Detector

Estos controles de Security Hub evalúan el servicio y los recursos de Amazon Fraud Detector.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[FraudDetector.1] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::FraudDetector::EntityType

Regla de AWS Config: frauddetector-entity-type-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un tipo de entidad de Amazon Fraud Detector tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el tipo de entidad no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el tipo de entidad no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un tipo de entidad de Amazon Fraud Detector (consola)

1. Abre la consola de Amazon Fraud Detector en <https://console.aws.amazon.com/frauddetect>.
2. En el panel de navegación, elija Entidades.
3. Seleccione un tipo de entidad de la lista.
4. En la sección de etiquetas de tipo de entidad, elija Administrar etiquetas.
5. Elija Añadir nueva etiqueta. Escriba la clave y el valor de para la etiqueta. Repita la acción para pares de clave-valor adicionales.
6. Cuando haya terminado de agregar etiquetas, elija Save (Guardar).

[FraudDetector.2] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::FraudDetector::Label`

Regla de AWS Config: `frauddetector-label-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una etiqueta de Amazon Fraud Detector tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si la etiqueta no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si la etiqueta no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una etiqueta de Amazon Fraud Detector (consola)

1. Abre la consola de Amazon Fraud Detector en <https://console.aws.amazon.com/frauddetect>.
2. En el panel de navegación, selecciona Etiquetas.
3. Seleccione una etiqueta de la lista.
4. En la sección de etiquetas y etiquetas, selecciona Administrar etiquetas.
5. Elija Añadir nueva etiqueta. Escriba la clave y el valor de para la etiqueta. Repita la acción para pares de clave-valor adicionales.
6. Cuando haya terminado de agregar etiquetas, elija Save (Guardar).

[FraudDetector.3] Los resultados de Amazon Fraud Detector deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::FraudDetector::Outcome

Regla de AWS Config : `frauddetector-outcome-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un resultado de Amazon Fraud Detector tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el resultado no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el resultado no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un resultado de Amazon Fraud Detector (consola)

1. Abre la consola de Amazon Fraud Detector en <https://console.aws.amazon.com/frauddetect>.
2. En el panel de navegación, seleccione Resultados.
3. Seleccione un resultado de la lista.
4. En la sección de etiquetas de resultados, selecciona Administrar etiquetas.
5. Elija Añadir nueva etiqueta. Escriba la clave y el valor de para la etiqueta. Repita la acción para pares de clave-valor adicionales.
6. Cuando haya terminado de agregar etiquetas, elija Save (Guardar).

[FraudDetector.4] Las variables de Amazon Fraud Detector deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::FraudDetector::Variable

Regla de AWS Config: `frauddetector-variable-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una variable de Amazon Fraud Detector tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si la variable no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si la variable no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una variable de Amazon Fraud Detector (consola)

1. Abre la consola de Amazon Fraud Detector en <https://console.aws.amazon.com/frauddetect>.
2. En el panel de navegación, elija Variables.
3. Seleccione una variable de la lista.
4. En la sección de etiquetas de variables, selecciona Administrar etiquetas.
5. Elija Añadir nueva etiqueta. Escriba la clave y el valor de para la etiqueta. Repita la acción para pares de clave-valor adicionales.
6. Cuando haya terminado de agregar etiquetas, elija Save (Guardar).

Controles de Security Hub para Amazon FSx

Estos AWS Security Hub controles evalúan el FSx servicio y los recursos de Amazon. Es posible que los controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[FSx.1] en el caso FSx de OpenZFS, los sistemas de archivos deben configurarse para copiar etiquetas en copias de seguridad y volúmenes

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::FSx::FileSystem

Regla de AWS Config : [fsx-openzfs-copy-tags-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un sistema de archivos Amazon FSx for OpenZFS está configurado para copiar etiquetas en copias de seguridad y volúmenes. Se produce un error en el control si el sistema de archivos de OpenZFS no está configurado para copiar etiquetas en copias de seguridad y volúmenes.

La identificación y el inventario de sus activos de TI es un aspecto importante de gobernanza y seguridad. Las etiquetas le ayudan a clasificar AWS los recursos de diferentes maneras, por ejemplo, por propósito, propietario o entorno. Esto es útil cuando tiene muchos recursos del mismo tipo porque puede identificar rápidamente un recurso específico en función de las etiquetas que le haya asignado.

Corrección

Para obtener información sobre cómo configurar un sistema de archivos OpenZFS FSx para copiar etiquetas en copias de seguridad y volúmenes, consulte [Actualización de un sistema de archivos](#) en la Guía del usuario de Amazon FSx para OpenZFS.

[FSx.2] FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad

Requisitos relacionados: NIST.800-53.r5 CP-9, NIST.800-53.r5 CM-8

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::FSx::FileSystem

Regla de AWS Config : [fsx-lustre-copy-tags-to-backups](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un sistema de archivos de Amazon FSx for Lustre está configurado para copiar etiquetas en copias de seguridad y volúmenes. Se produce un error en el control si el

sistema de archivos de Lustre no está configurado para copiar etiquetas en copias de seguridad y volúmenes.

La identificación y el inventario de sus activos de TI es un aspecto importante de gobernanza y seguridad. Las etiquetas le ayudan a clasificar AWS los recursos de diferentes maneras, por ejemplo, por propósito, propietario o entorno. Esto es útil cuando tiene muchos recursos del mismo tipo porque puede identificar rápidamente un recurso específico en función de las etiquetas que le haya asignado.

Corrección

Para obtener información sobre cómo configurar un sistema de archivos FSx para Lustre para copiar etiquetas a copias de seguridad, consulte [Copiar copias de seguridad dentro del mismo](#) sistema Cuenta de AWS en la Guía del usuario de Amazon FSx for Lustre.

[FSx.3] FSx para los sistemas de archivos OpenZFS, debe configurarse para el despliegue en zonas de disponibilidad múltiples

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::FSx::FileSystem

Regla de AWS Config : [fsx-openzfs-deployment-type-check](#)

Tipo de programa: Periódico

Parámetros: deploymentTypes: MULTI_AZ_1 (no personalizables)

Este control comprueba si un sistema de archivos Amazon FSx for OpenZFS está configurado para utilizar el tipo de despliegue de múltiples zonas de disponibilidad (Multi-AZ). El control falla si el sistema de archivos no está configurado para usar el tipo de implementación Multi-AZ.

Amazon FSx for OpenZFS admite varios tipos de implementación para sistemas de archivos: Multi-AZ (HA), Single-AZ (HA) y Single-AZ (no HA). Los tipos de implementación ofrecen diferentes niveles de disponibilidad y durabilidad. Los sistemas de archivos Multi-AZ (HA) se componen de un par de servidores de archivos de alta disponibilidad (HA) distribuidos en dos zonas de disponibilidad (AZs). Se recomienda utilizar el tipo de implementación Multi-AZ (HA) para la mayoría de las cargas de trabajo de producción debido al modelo de alta disponibilidad y durabilidad que ofrece.

Corrección

Puede configurar un sistema de archivos Amazon FSx for OpenZFS para que utilice el tipo de despliegue Multi-AZ al crear el sistema de archivos. No puede cambiar el tipo de implementación de un sistema de archivos existente FSx para OpenZFS.

Para obtener información sobre los tipos y opciones de implementación de los sistemas de archivos OpenZFS, consulte [Disponibilidad y durabilidad de Amazon FSx para OpenZFS y Administración de los recursos del sistema de archivos en](#) la Guía del usuario de Amazon FSx for OpenZFS. FSx

[FSx.4] FSx para los sistemas de archivos NetApp ONTAP, debe configurarse para el despliegue en zonas de disponibilidad múltiples

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::FSx::FileSystem

Regla de AWS Config : [fsx-ontap-deployment-type-check](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
deploymentTypes	Una lista de los tipos de implementación que se deben incluir en la evaluación. El control genera un FAILED resultado si un sistema de archivos no está configurado para usar un tipo de implementación especificado en la lista.	Enum	MULTI_AZ_1 , MULTI_AZ_2	MULTI_AZ_1 , MULTI_AZ_2

Este control comprueba si un sistema de archivos de Amazon FSx for NetApp ONTAP está configurado para utilizar un tipo de despliegue de varias zonas de disponibilidad (Multi-AZ). El control falla si el sistema de archivos no está configurado para usar un tipo de implementación Multi-AZ. Si lo desea, puede especificar una lista de tipos de implementación para incluirla en la evaluación.

Amazon FSx for NetApp ONTAP admite varios tipos de implementación para sistemas de archivos: Single-AZ 1, Single-AZ 2, Multi-AZ 1 y Multi-AZ 2. Los tipos de implementación ofrecen diferentes niveles de disponibilidad y durabilidad. Recomendamos utilizar un tipo de despliegue Multi-AZ para la mayoría de las cargas de trabajo de producción debido al modelo de alta disponibilidad y durabilidad que ofrecen los tipos de despliegue Multi-AZ. Los sistemas de archivos Multi-AZ admiten todas las características de disponibilidad y durabilidad de los sistemas de archivos Single-AZ. Además, están diseñados para proporcionar una disponibilidad continua de los datos incluso cuando una zona de disponibilidad (AZ) no esté disponible.

Corrección

No puedes cambiar el tipo de implementación de un sistema de archivos Amazon FSx for NetApp ONTAP existente. Sin embargo, puede hacer una copia de seguridad de los datos y, a continuación, restaurarlos en un nuevo sistema de archivos que utilice un tipo de despliegue Multi-AZ.

Para obtener información sobre los tipos y opciones de despliegue de los sistemas de archivos de ONTAP, consulte [Disponibilidad, durabilidad y opciones de despliegue y Gestión de los sistemas de archivos](#) en la Guía del usuario FSx de ONTAP. FSx

[FSx.5] FSx para Windows, los sistemas de archivos del servidor de archivos deben configurarse para el despliegue en zonas de disponibilidad múltiples

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::FSx::FileSystem

Regla de AWS Config : [fsx-windows-deployment-type-check](#)

Tipo de programa: Periódico

Parámetros: deploymentTypes: MULTI_AZ_1 (no personalizables)

Este control comprueba si un sistema de archivos del servidor de archivos de Amazon FSx para Windows está configurado para utilizar el tipo de despliegue de múltiples zonas de disponibilidad

(Multi-AZ). El control falla si el sistema de archivos no está configurado para usar el tipo de implementación Multi-AZ.

Amazon FSx para Windows File Server admite dos tipos de implementación para sistemas de archivos: Single-AZ y Multi-AZ. Los tipos de implementación ofrecen diferentes niveles de disponibilidad y durabilidad. Los sistemas de archivos Single-AZ se componen de una única instancia del servidor de archivos de Windows y un conjunto de volúmenes de almacenamiento dentro de una única zona de disponibilidad (AZ). Los sistemas de archivos Multi-AZ se componen de un clúster de servidores de archivos de Windows de alta disponibilidad repartidos en dos zonas de disponibilidad. Se recomienda utilizar el tipo de implementación Multi-AZ para la mayoría de las cargas de trabajo de producción debido al modelo de alta disponibilidad y durabilidad que ofrece.

Corrección

Puede configurar un sistema de archivos de Amazon FSx para Windows File Server para que utilice el tipo de despliegue Multi-AZ al crear el sistema de archivos. No puede cambiar el tipo de implementación de un sistema de archivos existente FSx para Windows File Server.

Para obtener información sobre los tipos y opciones de implementación de los sistemas de archivos de Windows File Server, consulte [Disponibilidad y durabilidad: sistemas de archivos Single-AZ y Multi-AZ](#) y [Introducción a Amazon FSx para Windows File Server](#) en la Guía del usuario de Amazon FSx para Windows File Server. FSx

Controles de Security Hub para Global Accelerator

Estos AWS Security Hub controles evalúan el AWS Global Accelerator servicio y los recursos.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[GlobalAccelerator.1] Los aceleradores de Global Accelerator deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::GlobalAccelerator::Accelerator

Regla de AWS Config : tagged-globalaccelerator-accelerator (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un AWS Global Accelerator acelerador tiene etiquetas con las teclas específicas definidas en el parámetro. `requiredTagKeys` El control lanza error si el acelerador no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el acelerador no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, incluidas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un acelerador global de Global Accelerator, consulte [Etiquetado en AWS Global Accelerator](#) en la Guía para desarrolladores de AWS Global Accelerator .

Controles de Security Hub para AWS Glue

Estos AWS Security Hub controles evalúan el AWS Glue servicio y los recursos. Es posible que los controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Glue.1] los AWS Glue trabajos deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Glue::Job

Regla de AWS Config : tagged-glue-job (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.		que cumplan con AWS los requisitos .	

Este control comprueba si un AWS Glue trabajo tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el trabajo no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el trabajo no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un AWS Glue trabajo, consulte las [AWS etiquetas AWS Glue en](#) la Guía del AWS Glue usuario.

[Glue.3] Las transformaciones AWS Glue de aprendizaje automático deben cifrarse en reposo

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::Glue::MLTransform

Regla de AWS Config : [glue-ml-transform-encrypted-at-rest](#)

Tipo de horario: provocado por un cambio

Parámetros: no

Este control comprueba si una transformación AWS Glue de aprendizaje automático está cifrada en reposo. El control falla si la transformación de machine learning no está cifrada en reposo.

Los datos en reposo hacen referencia a los datos que se almacenan en un almacenamiento persistente y no volátil durante cualquier periodo de tiempo. El cifrado de datos en reposo permite proteger la confidencialidad de los datos, lo que reduce el riesgo de que un usuario no autorizado pueda acceder a ellos.

Corrección

Para configurar el cifrado para las transformaciones de aprendizaje AWS Glue automático, consulte [Trabajar con transformaciones de aprendizaje automático](#) en la Guía del AWS Glue usuario.

[Glue.4] Los trabajos de AWS Glue Spark deberían ejecutarse en versiones compatibles de AWS Glue

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), niST.800-53.r5 CM-2, niST.800-53.r5 SI-2, niST.800-53.r5 SI-2 (2), niST.800-53.r5 SI-2 (4), Nlst.800-53.r5 SI-2 (5)

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: media

Tipo de recurso: `AWS::Glue::Job`

Regla de AWS Config : [glue-spark-job-supported-version](#)

Tipo de horario: provocado por un cambio

Parámetros **minimumSupportedGlueVersion: 3.0** (no personalizables)

Este control comprueba si un AWS Glue trabajo de Spark está configurado para ejecutarse en una versión compatible de AWS Glue. El control falla si el trabajo de Spark está configurado para ejecutarse en una versión anterior a la versión mínima compatible. AWS Glue

Note

Este control también genera la FAILED búsqueda de un AWS Glue trabajo de Spark si la propiedad AWS Glue version (`GlueVersion`) no existe o es nula en el elemento de configuración (CI) del trabajo. En esos casos, el hallazgo incluye la siguiente anotación: `GlueVersion is null or missing in glueetl job configuration`. Para abordar este tipo de FAILED hallazgo, añada la `GlueVersion` propiedad a la configuración del trabajo. Para obtener una lista de las versiones y los entornos de ejecución compatibles, consulte [AWS Glue las versiones](#) en la Guía del AWS Glue usuario.

Ejecutar trabajos de AWS Glue Spark en las versiones actuales de AWS Glue puede optimizar el rendimiento, la seguridad y el acceso a las funciones más recientes de AWS Glue. También puede ayudar a proteger contra las vulnerabilidades de seguridad. Por ejemplo, se podría lanzar una nueva versión para proporcionar actualizaciones de seguridad, solucionar problemas o introducir nuevas funciones.

Corrección

Para obtener información sobre cómo migrar un trabajo de Spark a una versión compatible de AWS Glue, consulte [Migración de trabajos AWS Glue de Spark](#) en la Guía del AWS Glue usuario.

Controles de Security Hub para Amazon GuardDuty

Estos AWS Security Hub controles de evalúan el GuardDuty servicio y los recursos de Amazon. Es posible que los controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[GuardDuty.1] GuardDuty debería estar activado

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), (4), NIST.800-53.r5 SA-1 1 (6) NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, 5 NIST.800-53.r5 CM-8(3), NIST.800-53.r5 RA-3 (2), NIST.800-53.r5 SA-1 5 (8), (19), (19), (19), (21), (25), (NIST.800-53.r5 SA-11), (3), NIST.800-53.r5 SA-1 NIST.800-53.r5 SA-8 Nist.800-53.r5 SI-20, NIST.800-53.r5 SA-8 Nist.800-53.r5 SI-4, NIST.800-53.r5 SC-5 Nist.800-53.r5, Nist.800-53.r5 R5 SI-4 NIST.800-53.r5 SC-5 NIST.800-53.r5 SC-5 (1), NiSt.800-53.r5 SI-4 (13), NiSt.800-53.r5 SI-4 (2), Nist.800-53.r5 SI-4 (25), Nist.800-53.r5 SI-4 (25), Nist.800-53.r5 SI-4 (5), NiSt.800-171.r2 3.4.2, NiSt.800-171.r2 3.14.6, NiSt.800-171.r2 3.14.7, PCI DSS v3.2.1/11.4 NIST.800-53.r5 SA-8 , PCI DSS v4.0.1/11.5.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: AWS : : : Account

Regla de AWS Config : [guardduty-enabled-centralized](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si Amazon GuardDuty está habilitado en tu GuardDuty cuenta y en tu región.

Se recomienda ampliamente que habilite GuardDuty en todas las AWS regiones de compatibles. Esto permite GuardDuty generar resultados sobre la actividad no autorizada o inusual incluso en las regiones que no usa de forma activa. Esto también permite GuardDuty monitorear CloudTrail eventos de global Servicios de AWS , como IAM.

Corrección

Para activarlo GuardDuty, consulta [Cómo empezar con GuardDuty](#) en la Guía del GuardDuty usuario de Amazon.

[GuardDuty.2] GuardDuty los filtros deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::GuardDuty::Filter`

Regla de AWS Config : `tagged-guardduty-filter` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un GuardDuty filtro de Amazon tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el filtro no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el filtro no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un GuardDuty filtro, consulta la referencia [TagResource](#) de la GuardDuty API de Amazon.

[GuardDuty.3] GuardDuty IPSets debe estar etiquetado

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::GuardDuty::IPSet

Regla de AWS Config : tagged-guardduty-ipset (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un Amazon GuardDuty IPSet tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si IPSet no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si `requiredTagKeys` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y lanza error si IPSet no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws :`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un GuardDuty IPSet, consulta la referencia [TagResource](#) de la GuardDuty API de Amazon.

[GuardDuty.4] GuardDuty los detectores deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::GuardDuty::Detector`

Regla de AWS Config : tagged-guardduty-detector (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si el GuardDuty detector de Amazon tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el detector no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el detector no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un GuardDuty detector, consulta la referencia [TagResource](#) de la GuardDuty API de Amazon.

[GuardDuty.5] La supervisión de registros de auditoría de GuardDuty EKS debe estar habilitada

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: `AWS::GuardDuty::Detector`

Regla de AWS Config : [guardduty-eks-protection-audit-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la supervisión de registros de auditoría de GuardDuty EKS está activada. En el caso de una cuenta independiente, el control falla si la supervisión de registros de auditoría de GuardDuty EKS está deshabilitada en la cuenta. En un entorno con varias cuentas, el control falla si ni la cuenta de GuardDuty administrador delegado ni ninguna de las cuentas de los miembros tienen habilitada la supervisión de registros de auditoría de EKS.

En un entorno con varias cuentas, el control genera resultados solo en la cuenta de GuardDuty administrador delegado. Solo el administrador delegado puede activar o desactivar la característica de la supervisión de registros de auditoría de EKS para las cuentas de los miembros en la organización. GuardDuty las cuentas de miembros no pueden modificar esta configuración desde sus cuentas. Este control genera FAILED resultados si el GuardDuty administrador delegado tiene una cuenta de miembro suspendida que no tiene habilitada la supervisión de registros de auditoría

de GuardDuty EKS. Para recibir un PASSED resultado, el administrador delegado debe desvincular estas cuentas suspendidas en GuardDuty

GuardDuty La supervisión de registros de auditoría de EKS lo ayuda a detectar actividades potencialmente sospechosas en los clústeres de Amazon Elastic Service (Amazon EKS). La supervisión de registros de auditoría de EKS utiliza los registros de auditoría de Kubernetes para capturar las actividades cronológicas de los usuarios, las aplicaciones que utilizan la API de Kubernetes y el plano de control.

Corrección

Para habilitar GuardDuty la supervisión de registros de auditoría de [EKS, consulte Supervisión de registros de auditoría](#) de EKS en la Guía del GuardDuty usuario de Amazon.

[GuardDuty.6] La protección de GuardDuty Lambda debe estar habilitada

Requisitos relacionados: PCI DSS v4.0.1/11.5.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: AWS::GuardDuty::Detector

Regla de AWS Config : [guardduty-lambda-protection-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la protección de GuardDuty Lambda está activada. En el caso de una cuenta independiente, el control falla si la protección de GuardDuty Lambda está deshabilitada en la cuenta. En un entorno con varias cuentas, el control lanza un error si ni la cuenta de GuardDuty administrador delegado ni ninguna de las cuentas de los miembros tienen habilitada la protección de Lambda.

En un entorno con varias cuentas, el control genera resultados solo en la cuenta de GuardDuty administrador delegado. Solo el administrador delegado puede activar o desactivar la característica de la protección de Lambda para las cuentas de los miembros en la organización. GuardDuty las cuentas de miembros no pueden modificar esta configuración desde sus cuentas. Este control genera FAILED resultados si el GuardDuty administrador delegado tiene una cuenta de miembro

suspendida que no tiene habilitada la protección de GuardDuty Lambda. Para recibir un PASSED resultado, el administrador delegado debe desvincular estas cuentas suspendidas en GuardDuty

GuardDuty La protección de Lambda le ayuda a identificar posibles amenazas de seguridad cuando se invoca una AWS Lambda función de. Después de activar la protección de Lambda, GuardDuty comienza a supervisar los registros de actividad de red de Lambda asociados a las funciones de Lambda de su. Cuenta de AWS Cuando una función de Lambda se invoca e GuardDuty identifica tráfico de red sospechoso que indica la presencia de un fragmento de código potencialmente malintencionado en su función de Lambda, GuardDuty genera un resultado.

Corrección

Para activar GuardDuty Lambda Protection, consulte Configuración de [Lambda Protection en la Guía del usuario](#) de Amazon. GuardDuty

[GuardDuty.7] La supervisión en tiempo de ejecución de GuardDuty EKS debe estar habilitada

Requisitos relacionados: PCI DSS v4.0.1/11.5.1

Categoría: Detectar - Servicios de detección

Gravedad: media

Tipo de recurso: AWS::GuardDuty::Detector

Regla de AWS Config : [guardduty-eks-protection-runtime-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la supervisión en tiempo de ejecución de GuardDuty EKS con administración automatizada de agentes está activada. En el caso de una cuenta independiente, el control lanza un error si la supervisión en tiempo de ejecución de GuardDuty EKS con administración automática de agentes está deshabilitada en la cuenta. En un entorno con varias cuentas, el control falla si ni la cuenta de GuardDuty administrador delegado ni ninguna de las cuentas de los miembros tienen habilitada la supervisión en tiempo de ejecución de EKS con administración automática de agentes.

En un entorno con varias cuentas, el control genera resultados solo en la cuenta de GuardDuty administrador delegado. Solo el administrador delegado puede activar o desactivar la característica

de la supervisión en tiempo de ejecución de EKS con administración automática de agentes para las cuentas de los miembros en la organización. GuardDuty las cuentas de miembros no pueden modificar esta configuración desde sus cuentas. Este control genera FAILED resultados si el GuardDuty administrador delegado tiene una cuenta de miembro suspendida que no tiene habilitada la supervisión en tiempo de ejecución de GuardDuty EKS. Para recibir un PASSED resultado, el administrador delegado debe desvincular estas cuentas suspendidas en GuardDuty.

La protección de EKS en Amazon GuardDuty proporciona una cobertura de detección de amenazas para ayudarlo a proteger los clústeres de Amazon EKS en su AWS entorno de. La supervisión en tiempo de ejecución de EKS utiliza los eventos de nivel de sistema operativo para ayudarlo a detectar posibles amenazas en los nodos y contenedores de EKS de sus clústeres de EKS.

Corrección

Para habilitar la supervisión en tiempo de ejecución de EKS con administración automática de agentes, consulte [Habilitar la supervisión en tiempo de GuardDuty ejecución](#) en la Guía del GuardDuty usuario de Amazon.

[GuardDuty.8] La protección contra GuardDuty malware para EC2 debe estar habilitada

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: AWS::GuardDuty::Detector

Regla de AWS Config : [guardduty-malware-protection-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la protección contra GuardDuty malware está activada. En el caso de una cuenta independiente, el control falla si la protección contra GuardDuty malware está deshabilitada en la cuenta. En un entorno con varias cuentas, el control lanza un error si ni la cuenta de GuardDuty administrador delegado ni ninguna de las cuentas de los miembros tienen habilitada la protección contra malware.

En un entorno con varias cuentas, el control genera resultados solo en la cuenta de GuardDuty administrador delegado. Solo el administrador delegado puede activar o desactivar la característica

de la protección contra malware para las cuentas de los miembros en la organización. GuardDuty las cuentas de miembros no pueden modificar esta configuración desde sus cuentas. Este control genera FAILED resultados si el GuardDuty administrador delegado tiene una cuenta de miembro suspendida que no tiene habilitada la protección contra GuardDuty malware. Para recibir un PASSED resultado, el administrador delegado debe desvincular estas cuentas suspendidas en GuardDuty

GuardDuty La protección contra malware para EC2 ayuda a detectar la presencia potencial de malware mediante el análisis de los volúmenes de Amazon Elastic Block Store (Amazon EBS) Block Store (EC2Amazon EBS)). La protección contra malware ofrece opciones de análisis en las que puede decidir si desea incluir o excluir EC2 instancias y cargas de trabajo de contenedores específicas en el momento del análisis. También ofrece la opción de retener las instantáneas de los volúmenes de EBS adjuntos a las EC2 instancias o cargas de trabajo de contenedores en sus cuentas. GuardDuty Las instantáneas se conservan solo cuando se encuentra malware y se generan los resultados de la protección contra malware.

Corrección

Para activar la protección contra GuardDuty malware EC2, consulte [Configuración del análisis GuardDuty de malware iniciado](#) en la Guía del GuardDuty usuario de Amazon.

[GuardDuty.9] La protección de GuardDuty RDS debe estar habilitada

Requisitos relacionados: PCI DSS v4.0.1/11.5.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: AWS::GuardDuty::Detector

Regla de AWS Config : [guardduty-rds-protection-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la protección GuardDuty de RDS está activada. En el caso de una cuenta independiente, el control falla si la protección de GuardDuty RDS está deshabilitada en la cuenta. En un entorno con varias cuentas, el control lanza un error si ni la cuenta de GuardDuty administrador delegado ni ninguna de las cuentas de los miembros tienen habilitada la protección de RDS.

En un entorno con varias cuentas, el control genera resultados solo en la cuenta de GuardDuty administrador delegado. Solo el administrador delegado puede activar o desactivar la característica de la protección de RDS para las cuentas de los miembros en la organización. GuardDuty las cuentas de miembros no pueden modificar esta configuración desde sus cuentas. Este control genera FAILED resultados si el GuardDuty administrador delegado tiene una cuenta de miembro suspendida que no tiene habilitada la protección de GuardDuty RDS. Para recibir un PASSED resultado, el administrador delegado debe desvincular estas cuentas suspendidas en GuardDuty.

La protección de RDS en GuardDuty analiza y perfila la actividad de inicio de sesión en RDS para detectar posibles amenazas de acceso a sus bases de datos de Amazon Aurora (Aurora edición compatible con MySQL y Aurora edición compatible con PostgreSQL). Esta característica le permite identificar comportamientos de inicio de sesión potencialmente sospechosos. La protección de RDS no requiere infraestructura adicional; está diseñada para no afectar al rendimiento de las instancias de bases de datos. Cuando la protección de RDS detecta un intento de inicio de sesión sospechoso o anómalo que implica una amenaza para su base de datos, GuardDuty genera un nuevo resultado con detalles de la base de datos que está potencialmente afectada.

Corrección

Para activar la protección de GuardDuty RDS, consulte Protección de [GuardDuty RDS en la](#) Guía GuardDuty del usuario de Amazon.

[GuardDuty.10] La protección de GuardDuty S3 debe estar habilitada

Requisitos relacionados: PCI DSS v4.0.1/11.5.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: AWS::GuardDuty::Detector

Regla de AWS Config : [guardduty-s3-protection-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la protección de GuardDuty S3 está activada. En el caso de una cuenta independiente, el control falla si la protección de GuardDuty S3 está deshabilitada en la cuenta. En

un entorno con varias cuentas, el control lanza un error si ni la cuenta de GuardDuty administrador delegado ni ninguna de las cuentas de los miembros tienen habilitada la protección de S3.

En un entorno con varias cuentas, el control genera resultados solo en la cuenta de GuardDuty administrador delegado. Solo el administrador delegado puede activar o desactivar la característica de la protección de S3 para las cuentas de los miembros en la organización. GuardDuty las cuentas de miembros no pueden modificar esta configuración desde sus cuentas. Este control genera FAILED resultados si el GuardDuty administrador delegado tiene una cuenta de miembro suspendida que no tiene habilitada la protección de GuardDuty S3. Para recibir un PASSED resultado, el administrador delegado debe desvincular estas cuentas suspendidas en GuardDuty

La protección de S3 GuardDuty permite supervisar las operaciones de la API de nivel de objeto para identificar los posibles riesgos de seguridad para los datos de los buckets de Amazon Simple Storage Service (Amazon S3). GuardDuty supervisa las amenazas contra los recursos de S3 mediante el análisis AWS CloudTrail de eventos de administración de y eventos de datos de CloudTrail S3.

Corrección

Para activar la protección GuardDuty S3, consulte [Amazon S3 Protection en Amazon GuardDuty](#) en la Guía del GuardDuty usuario de Amazon.

[GuardDuty.11] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: AWS::GuardDuty::Detector

Regla de AWS Config : [guardduty-runtime-monitoring-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la supervisión en tiempo de ejecución está activada en Amazon GuardDuty. En el caso de una cuenta independiente, el control falla si la supervisión en GuardDuty tiempo de ejecución está deshabilitada para la cuenta. En un entorno con varias cuentas, el control lanza un error si la supervisión en GuardDuty tiempo de ejecución está deshabilitada para la cuenta de GuardDuty administrador delegado y todas las cuentas de los miembros.

En un entorno con varias cuentas, solo el GuardDuty administrador delegado puede habilitar o desactivar la supervisión en GuardDuty tiempo de ejecución para las cuentas de su organización. Además, solo el GuardDuty administrador puede configurar y administrar los agentes de seguridad que GuardDuty utiliza para la supervisión en tiempo de ejecución de AWS las cargas de trabajo y los recursos de las cuentas de la organización. GuardDuty las cuentas de los miembros no pueden activar, configurar ni deshabilitar Runtime Monitoring para sus propias cuentas.

GuardDuty La supervisión en tiempo de ejecución observa y analiza los eventos de archivos, redes y sistemas operativos para ayudarlo a detectar posibles amenazas en AWS cargas de trabajo específicas de en su entorno. Utiliza agentes GuardDuty de seguridad que aportan 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. Puede habilitar y administrar el agente de seguridad para cada tipo de recurso que desee supervisar para detectar posibles amenazas, como los clústeres de Amazon EKS y las EC2 instancias de Amazon.

Corrección

Para obtener información sobre cómo configurar y habilitar GuardDuty Runtime Monitoring, consulte [GuardDuty Runtime Monitoring](#) y [Enabling GuardDuty Runtime Monitoring](#) en la Guía del GuardDuty usuario de Amazon.

[GuardDuty.12] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada

Categoría: Detectar - Servicios de detección

Gravedad: media

Tipo de recurso: AWS::GuardDuty::Detector

Regla de AWS Config : [guardduty-ecs-protection-runtime-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el agente de seguridad GuardDuty automatizado de Amazon está activado para la supervisión en tiempo de ejecución de los clústeres de Amazon ECS AWS Fargate. En el caso de una cuenta independiente, el control falla si el agente de seguridad está deshabilitado para la cuenta. En un entorno con varias cuentas, el control lanza un error si el agente de seguridad

está desactivado para la cuenta de GuardDuty administrador delegado y todas las cuentas de los miembros.

En un entorno con varias cuentas, este control genera resultados solo en la cuenta de GuardDuty administrador delegado. Esto se debe a que solo el GuardDuty administrador delegado puede habilitar o deshabilitar la supervisión en tiempo de ejecución de los recursos de ECS-Fargate para las cuentas de su organización. GuardDuty las cuentas de miembros no pueden hacer esto para sus propias cuentas. Además, este control genera FAILED resultados si GuardDuty se suspende para una cuenta de miembro y la supervisión del tiempo de ejecución de los recursos de ECS-Fargate está deshabilitada para la cuenta de miembro. Para recibir una confirmación PASSED, el GuardDuty administrador debe desvincular la cuenta de miembro suspendida de su cuenta de administrador mediante GuardDuty

GuardDuty La supervisión en tiempo de ejecución observa y analiza los eventos de archivos, redes y sistemas operativos para ayudarlo a detectar posibles amenazas en AWS cargas de trabajo específicas de su entorno. Utiliza agentes GuardDuty de seguridad que aportan 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. Puede habilitar y administrar el agente de seguridad para cada tipo de recurso que desee supervisar en busca de posibles amenazas. Esto incluye los clústeres de Amazon ECS activados AWS Fargate.

Corrección

Para habilitar y administrar el agente de seguridad para la supervisión en tiempo de GuardDuty ejecución de los recursos de ECS-Fargate, debe usarlo directamente. GuardDuty No puede habilitarlo ni administrarlo manualmente para los recursos de ECS-Fargate. Para obtener información sobre cómo habilitar y administrar el agente de seguridad, consulte [Requisitos previos para el soporte AWS Fargate \(solo para Amazon ECS\)](#) y [Administración del agente de seguridad automatizado para AWS Fargate \(solo Amazon ECS\)](#) en la Guía del GuardDuty usuario de Amazon.

[GuardDuty.13] La monitorización del GuardDuty EC2 tiempo de ejecución debe estar habilitada

Categoría: Detectar - Servicios de detección

Gravedad: media

Tipo de recurso: AWS::GuardDuty::Detector

Regla de AWS Config : [guardduty-ec2-protection-runtime-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el agente de seguridad GuardDuty automatizado de Amazon está habilitado para la supervisión en tiempo de ejecución de las EC2 instancias de Amazon. En el caso de una cuenta independiente, el control falla si el agente de seguridad está deshabilitado para la cuenta. En un entorno con varias cuentas, el control lanza un error si el agente de seguridad está desactivado para la cuenta de GuardDuty administrador delegado y todas las cuentas de los miembros.

En un entorno con varias cuentas, este control genera resultados solo en la cuenta de GuardDuty administrador delegado. Esto se debe a que solo el GuardDuty administrador delegado puede activar o desactivar Runtime Monitoring de las EC2 instancias de Amazon para las cuentas de su organización. GuardDuty las cuentas de miembros no pueden hacer esto para sus propias cuentas. Además, este control genera FAILED resultados si GuardDuty se suspende la cuenta de un miembro y si se inhabilita la supervisión del tiempo de ejecución de las EC2 instancias en esa cuenta. Para recibir una confirmación PASSED, el GuardDuty administrador debe desvincular la cuenta de miembro suspendida de su cuenta de administrador mediante GuardDuty.

GuardDuty La supervisión en tiempo de ejecución observa y analiza los eventos de archivos, redes y sistemas operativos para ayudarlo a detectar posibles amenazas en AWS cargas de trabajo específicas de su entorno. Utiliza agentes GuardDuty de seguridad que aportan 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. Puede habilitar y administrar el agente de seguridad para cada tipo de recurso que desee supervisar en busca de posibles amenazas. Esto incluye las EC2 instancias de Amazon.

Corrección

Para obtener información sobre la configuración y la administración del agente de seguridad automatizado para la supervisión en tiempo de GuardDuty ejecución de EC2 las instancias, consulte [Requisitos previos para el soporte de EC2 instancias de Amazon](#) y [Habilitar el agente de seguridad automatizado para EC2 las instancias de Amazon](#) en la Guía del GuardDuty usuario de Amazon.

Controles de Security Hub AWS Identity and Access Management

Estos AWS Security Hub controles de evalúan el servicio y los recursos de AWS Identity and Access Management (IAM). Es posible que los controles de no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[IAM.1] Las políticas de IAM no deben permitir privilegios administrativos completos “*”

Requisitos relacionados: Indicador de AWS referencia de CIS v1.2.0/1.22, Indicador de referencia de CIS AWS v1.4.0/1.16 NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 Indicador de referencia de CIS v1.4.0/1.16, NIST.800-53.r5 AC-3 NIST.800-171.r2 NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6 3.1.4, NIST.800-53.r5 AC-6 PCI DSS NIST.800-53.r5 AC-6 v3.2.1/7.2.1 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6

Categoría: Proteger - Administración de acceso seguro

Gravedad: alta

Tipo de recurso: AWS::IAM::Policy

Regla de AWS Config : [iam-policy-no-statements-with-admin-access](#)

Tipo de horario: provocado por un cambio

Parámetros:

- `excludePermissionBoundaryPolicy: true` (no personalizable)

Este control comprueba si la versión predeterminada de las políticas de IAM (también conocidas como políticas administradas por el cliente) tiene acceso de administrador con una instrucción que tenga "Effect": "Allow" con "Action": "*" en "Resource": "*". El control falla si tiene políticas de IAM con una declaración de este tipo.

El control solo comprueba las políticas administradas por el cliente que haya creado usted. No comprueba las políticas en línea ni las AWS administradas por.

Las políticas de IAM definen un conjunto de privilegios concedidos a usuarios, grupos o roles. Siguiendo los consejos de seguridad estándar, AWS recomienda conceder privilegios mínimos, lo que significa conceder únicamente los permisos obligatorios para realizar una tarea. Cuando proporciona privilegios administrativos completos en lugar del conjunto mínimo de permisos que necesita el usuario, expone los recursos a acciones potencialmente no deseadas.

En lugar de concederles privilegios administrativos totales, determine las tareas que tienen que realizar los usuarios y elabore políticas al respecto para permitir a los usuarios realizar solo esas tareas. Es más seguro comenzar con un conjunto mínimo de permisos y conceder permisos adicionales según sea necesario. No comience con permisos demasiado indulgentes para luego restringirlos más adelante.

Debe quitar las políticas de IAM que tienen una instrucción con "Effect": "Allow" y "Action": "*" en "Resource": "*".

 Note

AWS Config debe habilitarse en todas las regiones en las que se utiliza Security Hub. Sin embargo, el registro de recursos globales se puede habilitar en una sola región. Si solo registra recursos globales en una única región, puede desactivar este control en todas las regiones salvo aquella en la que haya registrado los recursos globales.

Corrección

Para modificar sus políticas de IAM de manera que no permitan todos los privilegios administrativos "*", consulte [Edición de políticas de IAM](#) en la Guía del usuario de IAM.

[IAM.2] Los usuarios de IAM no deben tener políticas de IAM asociadas

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/1.15, CIS AWS Foundations Benchmark v1.2.0/1.16, NIST.800-53.r5 AC-2 (1), (15), (7), (3) NIST.800-53.r5 AC-2, NIST.800-171.r2 3.1.1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 NIST.800-171.r2 3.1.2, NIST.800-53.r5 AC-3 NIST.800-171.r2 3.1.7 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 NIST.800-171.r2 3.3.9, NIST.800-171.r2 3.13.3, PCI DSS v3.2.1/7.2.1

Categoría: Proteger - Administración de acceso seguro

Gravedad: baja

Tipo de recurso: AWS::IAM::User

Regla de AWS Config : [iam-user-no-policies-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si sus usuarios de IAM tienen políticas asociadas. El control falla si los usuarios de IAM tienen políticas asociadas. Los usuarios de IAM deben heredar los permisos de los grupos de IAM o asumir un rol.

De forma predeterminada, los usuarios, grupos y roles de IAM no tienen acceso a AWS los recursos de. Las políticas de IAM conceden privilegios a los usuarios, grupos o roles. Recomendamos aplicar

políticas de IAM directamente a grupos y roles, pero no a los usuarios. La asignación de privilegios en el nivel de grupo o rol reduce la complejidad de la administración del acceso a medida que crece el número de usuarios. A su vez, la reducción de la complejidad de la administración del acceso podría reducir la oportunidad de que una entidad principal reciba o conserve accidentalmente excesivos privilegios.

 Note

AWS Config debe habilitarse en todas las regiones en las que se utiliza Security Hub. Sin embargo, el registro de recursos globales se puede habilitar en una sola región. Si solo registra recursos globales en una única región, puede deshabilitar este control en todas las regiones salvo en la región en la que haya registrado los recursos globales.

Corrección

Para resolver este problema, [cree un grupo de IAM](#) y asocie la política al grupo. Luego, [agregue los usuarios al grupo](#). La política se aplica a cada usuario del grupo. Para eliminar una política asociada directamente a un usuario, consulte [Adición y eliminación de permisos de identidad de IAM](#) en la Guía del usuario de IAM.

[IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos

Requisitos relacionados: Indicador de referencia de CIS AWS v3.0.0/1.14, Indicador de referencia de CIS v1.4.0/1.14, AWS Indicador de referencia de CIS v1.2.0/1.4, NIST.800-53.r5 AC-2 (1), (3), (15), PCI AWS DSS v4.0.1/8.3.9, PCI DSS NIST.800-53.r5 AC-2 v4.0.1/8.6.3 NIST.800-53.r5 AC-3

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS::IAM::User

Regla de AWS Config : [access-keys-rotated](#)

Tipo de programa: Periódico

Parámetros:

- `maxAccessKeyAge`: 90 (no personalizable)

Este control comprueba si las claves de acceso activas rotan en un plazo de 90 días.

Le recomendamos encarecidamente que no genere y elimine todas las claves de acceso de la cuenta. En su lugar, la práctica recomendada es crear uno o más roles de IAM o utilizar la [federación](#) a través AWS IAM Identity Center de. Puede utilizar estos métodos para permitir que sus usuarios accedan a AWS Management Console y AWS CLI.

Cada enfoque tiene sus casos de uso. La federación es generalmente mejor para las empresas que tienen un directorio o plan central existente y prevén que van a necesitar más que el límite actual de usuarios de IAM. Las aplicaciones que se ejecutan fuera de un AWS entorno de necesitan claves de acceso para el acceso programático a AWS los recursos.

Sin embargo, si los recursos que necesitan acceso programático se ejecutan internamente AWS, la mejor práctica es utilizar las funciones de IAM. Los roles le permiten conceder acceso a un recurso sin codificar de forma rígida un ID de clave de acceso y una clave de acceso secreta en la configuración.

Para obtener más información sobre cómo proteger las claves de acceso y la cuenta, consulte [las prácticas recomendadas para administrar las claves de AWS acceso](#) en el. Referencia general de AWS Consulte también la publicación del blog [Pautas a seguir para proteger su Cuenta de AWS mientras utiliza el acceso mediante programación](#).

Si ya tiene una clave de acceso, Security Hub recomienda que rote las claves de acceso cada 90 días. La rotación de las claves de acceso reduce la posibilidad de que se utilice una clave de acceso asociada a una cuenta en peligro o cancelada. También garantiza que no se pueda acceder a los datos con una clave antigua que podría haberse perdido, revelado o robado. Actualice siempre sus aplicaciones después de rotar las claves de acceso.

Las claves de acceso constan de un ID de clave de acceso y de una clave de acceso secreta. Se utilizan para firmar las solicitudes programáticas que realiza a AWS. Los usuarios necesitan sus propias claves de acceso para realizar llamadas mediante programación a AWS desde la AWS CLI, las herramientas para Windows PowerShell AWS SDKs, la o las llamadas HTTP directas a través de las operaciones de API de individual Servicios de AWS.

Si la organización utiliza AWS IAM Identity Center (IAM Identity Center), los usuarios pueden iniciar sesión en Active Directory, en un directorio de IAM [Identity Center de IAM Identity Center](#). A continuación, se pueden asignar a un rol de IAM de IAM que les permita ejecutar AWS CLI

comandos o llamar a las AWS API de sin necesidad de claves de acceso. Para obtener más información, consulte [Configuración del AWS CLI uso AWS IAM Identity Center](#) en la Guía del AWS Command Line Interface usuario.

 Note

AWS Config debe habilitarse en todas las regiones en las que se utiliza Security Hub. Sin embargo, el registro de recursos globales se puede habilitar en una sola región. Si solo registra recursos globales en una única región, puede desactivar este control en todas las regiones salvo aquella en la que haya registrado los recursos globales.

Corrección

Para rotar las claves de acceso que tienen más de 90 días de antigüedad, consulte [Rotación de las claves de acceso](#) en la Guía del usuario de IAM. Siga las instrucciones para cualquier usuario cuya clave de acceso tenga más de 90 días de antigüedad.

[IAM.4] La clave de acceso del usuario raíz de IAM no debería existir

Requisitos relacionados: Indicador de referencia de CIS AWS v3.0.0/1.4, Indicador de referencia de CIS v1.4.0/1.4, Indicador de referencia de CIS AWS AWS Foundations Benchmark v1.2.0/1.12, PCI DSS v3.2.1/2.1, PCI DSS v3.2.1/2.2, PCI DSS v3.2.1/7.2.1, (1), (1), (7), (10), (2) NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6

Categoría: Proteger - Administración de acceso seguro

Gravedad: crítica

Tipo de recurso: AWS :: Account

Regla de AWS Config : [iam-root-access-key-check](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si está presente la clave de acceso del usuario raíz.

El usuario raíz es el usuario con más privilegios de Cuenta de AWS. AWS las claves de acceso ofrecen acceso mediante programación a una cuenta determinada.

Security Hub recomienda quitar todas las claves de acceso asociadas al usuario raíz. Esto limita los vectores que se pueden utilizar para comprometer su cuenta. También fomenta la creación y el uso de cuentas basadas en roles, que tienen menos privilegios.

Corrección

Para eliminar la clave de acceso del usuario raíz, consulte [Eliminar las claves de acceso del usuario raíz](#) en la Guía del usuario de IAM. Para eliminar las claves de acceso del usuario raíz de una Cuenta de AWS en AWS GovCloud (US), consulte [Eliminar las claves de acceso del usuario raíz de mi AWS GovCloud \(US\) cuenta](#) en la Guía del AWS GovCloud (US) usuario de.

[IAM.5] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola

Requisitos relacionados: Indicador de referencia de CIS AWS v3.0.0/1.10, Indicador de referencia de CIS v1.4.0/1.10, Indicador de referencia de CIS AWS v1.2.0/1.2, (1), (15), NIST.800-53.r5 AC-2 (1), (2), (2), (2), (6), (2), (6), (2), (6), (2), (6), (2), (6), NIST.800-53.r5 AC-3 (2), (6), (2), NIST.800-53.r5 IA-2 (6), (8), PCI AWS DSS NIST.800-53.r5 IA-2 v4.0.1/8.4.2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS::IAM::User

Regla de AWS Config : [mfa-enabled-for-iam-console-access](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la autenticación AWS multifactor (MFA) está habilitada para todos los usuarios de IAM de IAM que utilizan una contraseña de consola.

La autenticación multifactor (MFA) agrega una capa adicional de protección además del nombre de usuario y la contraseña. Si la MFA está habilitada, cuando un usuario inicia sesión en un AWS sitio web, se le pide que indique su nombre de usuario y contraseña. Además, se les solicita un código de autenticación desde su dispositivo AWS MFA.

Recomendamos que habilite la MFA para todas las cuentas que tengan una contraseña de consola. MFA está diseñado para proporcionar una mayor seguridad para acceder a la consola. La entidad

de autenticación debe poseer un dispositivo que emita una clave sujeta a limitación temporal y debe tener conocimiento de una credencial.

 Note

AWS Config debe habilitarse en todas las regiones en las que se utiliza Security Hub. Sin embargo, el registro de recursos globales se puede habilitar en una sola región. Si solo registra recursos globales en una única región, puede desactivar este control en todas las regiones salvo aquella en la que haya registrado los recursos globales.

Corrección

Para agregar MFA a los usuarios de IAM, consulte [Uso de la autenticación multifactor \(MFA\) en AWS](#) en la Guía del usuario de IAM.

Ofrecemos una clave de seguridad MFA gratuita a los clientes que reúnan los requisitos. [Compruebe si cumple los requisitos y solicite su clave gratuita.](#)

[PCI.IAM.6] La MFA de hardware debe estar habilitada para el usuario raíz

Requisitos relacionados: Indicador de referencia de CIS AWS v3.0.0/1.6, Indicador de referencia de CIS AWS v1.4.0/1.6, Indicador de referencia de CIS v1.2.0/1.14, CIS AWS Foundations Benchmark v3.2.1/8.3.1, (1), (15), (1), (1), NIST.800-53.r5 AC-2 (1), (2), NIST.800-53.r5 AC-3 PCI DSS v4.0.1/8.4.2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2

Categoría: Proteger - Administración de acceso seguro

Gravedad: crítica

Tipo de recurso: AWS :: Account

Regla de AWS Config : [root-account-hardware-mfa-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si Cuenta de AWS está habilitada para usar un dispositivo de hardware de autenticación multifactor (MFA) para iniciar sesión con credenciales de usuario raíz. El control falla

si la MFA de hardware no está habilitada o si se permite que los dispositivos MFA virtuales inicien sesión con credenciales de usuario raíz.

Una aplicación de MFA virtual podría no proporcionar el mismo nivel de seguridad que un dispositivo MFA físico. Recomendamos que utilice un dispositivo MFA virtual solo mientras espera la aprobación de compra de hardware o la llegada de su hardware. Para obtener más información, consulte [Asignar un dispositivo MFA virtual \(consola\)](#) en la Guía del usuario de IAM.

 Note

Security Hub evalúa este control en función de la presencia de credenciales de usuario raíz (perfil de inicio de sesión) en un Cuenta de AWS. El control arroja resultados PASSED en los siguientes casos:

- Las credenciales de usuario raíz están presentes en la cuenta y la MFA del hardware está habilitada para el usuario raíz.
- Las credenciales de usuario raíz no están presentes en la cuenta.

El control genera una FAILED búsqueda si las credenciales del usuario raíz están presentes en la cuenta y el MFA de hardware no está habilitado para el usuario raíz.

Corrección

Para obtener información sobre cómo habilitar la MFA de hardware para el usuario raíz, consulte [Autenticación multifactorial Usuario raíz de la cuenta de AWS en la Guía](#) del usuario de IAM.

Ofrecemos una clave de seguridad MFA gratuita a los clientes que reúnan los requisitos. Para determinar si reúne los requisitos, consulte el Programa de [claves de seguridad de MFA](#). FAQs

[IAM.7] Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), (3), (1), NIST.800-53.r5 AC-2 NIST.800-171.r2 3.5.2, NIST.800-53.r5 AC-3 NIST.800-171.r2 3.5.7, NIST.800-171.r2 3.5.8, NIST.800-171.r2 3.5.9, PCI DSS v4.0.1/8.3.6, PCI DSS v4.0.1/8.3.7 NIST.800-53.r5 IA-5

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS:::Account

Regla de AWS Config : [iam-password-policy](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
RequireUppercaseCharacters	Requiere que al menos haya un carácter en mayúscula en la contraseña	Booleano	true o false	true
RequireLowercaseCharacters	Requiere que al menos haya un carácter en minúscula en la contraseña	Booleano	true o false	true
RequireSymbols	Requiere que al menos haya un símbolo en la contraseña	Booleano	true o false	true
RequireNumbers	Requiere que al menos haya un número en la contraseña	Booleano	true o false	true
MinimumPasswordLength	Cantidad mínima de caracteres en la contraseña	Entero	De 8 a 128	8
PasswordReusePrevention	Cantidad de rotaciones de contraseñas para poder reutilizar una contraseña anterior	Entero	De 12 a 24	Sin valor predeterminado
MaxPasswordAge	Cantidad de días antes de que la contraseña expire	Entero	De 1 a 90	Sin valor predeterminado

Este control comprueba si la política de contraseñas de cuenta para usuarios de IAM utiliza las siguientes configuraciones seguras. Se producirá un error en el control si la política de contraseñas no utiliza configuraciones seguras. A menos que proporcione valores personalizados de parámetros, Security Hub utiliza los valores predeterminados que se mencionan en la tabla anterior. Los parámetros PasswordReusePrevention y MaxPasswordAge no tienen un valor predeterminado, por lo que, si los excluye, Security Hub ignora la cantidad de rotaciones de contraseñas y la antigüedad de la contraseña al evaluar este control.

Para obtener acceso a AWS Management Console, los usuarios de IAM necesitan contraseñas. Como práctica recomendada, Security Hub recomienda encarecidamente que, en lugar de crear usuarios de IAM, utilice la federación. La federación permite a los usuarios utilizar sus credenciales corporativas existentes para iniciar sesión en AWS Management Console. Utilice AWS IAM Identity Center (IAM Identity Center) para crear o federar el usuario y, a continuación, asuma una rol de IAM en una cuenta.

Para obtener más información sobre los proveedores de identidad y la federación, consulte [Proveedores de identidad y federación](#) en la Guía del usuario de IAM. Para obtener más información sobre IAM Identity Center, consulte la [AWS IAM Identity Center Guía del usuario](#).

Si necesita utilizar usuarios de IAM, Security Hub recomienda que exija la creación de contraseñas de usuario seguras. Puede establecer una política de contraseñas en la Cuenta de AWS para especificar los requisitos de complejidad y los periodos de rotación obligatorios de las contraseñas. Al crear o cambiar una política de contraseñas, la mayoría de los ajustes de la política de contraseñas se aplican la siguiente vez que los usuarios cambien sus contraseñas. Algunos de los ajustes se aplican de forma inmediata.

Corrección

Para actualizar la política de contraseñas, consulte [Configuración de una política de contraseñas de la cuenta para usuarios de IAM](#) en la Guía del usuario de IAM.

[IAM.8] Deben eliminarse las credenciales de usuario de IAM no utilizadas

Requisitos relacionados: Indicador de referencia de AWS CIS v1.2.0/1.3, NIST.800-53.r5 AC-2 (1), (3) NIST.800-53.r5 AC-2, (15), (15), NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 NIST.800-171.r2 3.1.2, PCI DSS v3.2.1/8.1.4 NIST.800-53.r5 AC-6, PCI DSS v4.0.1/8.2.6

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS::IAM::User

Regla de AWS Config : [iam-user-unused-credentials-check](#)

Tipo de programa: Periódico

Parámetros:

- maxCredentialUsageAge: 90 (no personalizable)

Este control comprueba si los usuarios de IAM tienen contraseñas o claves de acceso activas que no se han utilizado durante 90 días.

Los usuarios de IAM pueden acceder a AWS los recursos de utilizando diferentes tipos de credenciales, como contraseñas o claves de acceso.

Security Hub recomienda que elimine o desactive todas las credenciales que han dejado de utilizarse durante 90 días o más. Al deshabilitar o eliminar credenciales innecesarias se reduce la oportunidad de que se utilicen credenciales asociadas a una cuenta en peligro o abandonada.

Note

AWS Config debe habilitarse en todas las regiones en las que se utiliza Security Hub. Sin embargo, el registro de recursos globales se puede habilitar en una sola región. Si solo registra recursos globales en una única región, puede desactivar este control en todas las regiones salvo aquella en la que haya registrado los recursos globales.

Corrección

Al ver la información del usuario en la consola de IAM, hay columnas para la antigüedad de la clave de acceso, la antigüedad de la Contraseña y la Última actividad. Si el valor en cualquiera de estas columnas es superior a 90 días, desactive las credenciales de esos usuarios.

También puede utilizar los [informes de credenciales](#) para monitorizar a los usuarios e identificar a aquellos que no tienen actividad durante 90 días o más. Puede descargar los informes de credenciales en formato .csv desde la consola de IAM.

Después de identificar las cuentas inactivas o las credenciales no utilizadas, desactívalas. Para obtener instrucciones, consulte [Creación, cambio o eliminación de la contraseña de un usuario de IAM \(consola\)](#) en la Guía del usuario de IAM.

[IAM.9] La MFA debe estar habilitada para el usuario raíz

Requisitos relacionados: PCI DSS v3.2.1/8.3.1, PCI DSS v4.0.1/8.4.2, CIS Foundations Benchmark v3.0.0/1.5, Indicador de referencia de CIS v1.4.0/1.5, Indicador de referencia de CIS v1.2.0/1.13, CIS AWS Foundations Benchmark v1.2.0/1.13, CIS Foundations Benchmark v1.2.0/1.13, CIS AWS Foundations Benchmark v1.2.0/1.13, CIS AWS Foundations Benchmark v1.2.0/1.13, (2), (6), (8) NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2

Categoría: Proteger - Administración de acceso seguro

Gravedad: crítica

Tipo de recurso: AWS :: Account

Regla de AWS Config : [root-account-mfa-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la autenticación multifactor (MFA) de está habilitada para que el usuario raíz de Cuenta de AWS IAM inicie sesión en. AWS Management Console Se produce un error en el control si la MFA no está habilitada para el usuario raíz de la cuenta.

El usuario raíz de IAM Cuenta de AWS tiene acceso completo a todos los servicios y recursos de de la cuenta. Si la MFA está habilitada, el usuario debe introducir un nombre de usuario, una contraseña y un código de autenticación desde su dispositivo de AWS MFA para poder iniciar sesión en. AWS Management Console La MFA añade una capa adicional de protección además de un nombre de usuario y una contraseña.

Este control arroja PASSED resultados en los siguientes casos:

- Las credenciales de usuario raíz están presentes en la cuenta y la MFA está habilitada para el usuario raíz.
- Las credenciales de usuario raíz no están presentes en la cuenta.

El control genera FAILED resultados si las credenciales del usuario raíz están presentes en la cuenta y el MFA no está habilitado para el usuario raíz.

Corrección

Para obtener información sobre cómo habilitar la MFA para el usuario raíz de un dispositivo Cuenta de AWS, consulte [Autenticación multifactorial Usuario raíz de la cuenta de AWS en la Guía del usuario.AWS Identity and Access Management](#)

[IAM.10] Las políticas de contraseñas de usuarios de IAM deben tener configuraciones seguras

Requisitos relacionados: NIST.800-171.r2 3.5.2, NIST.800-171.r2, NIST.800-171.r2 3.5.8, NIST.800-171.r2 3.2.1/8.1.4, PCI DSS v3.2.1/8.1.4, PCI DSS v3.2.1/8.2.3, PCI DSS v3.2.1/8.2.5

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS:::Account

Regla de AWS Config : [iam-password-policy](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si la política de contraseñas de cuenta para usuarios de IAM utiliza las siguientes configuraciones mínimas de PCI DSS.

- **RequireUppercaseCharacters:** requiere que al menos haya un carácter en mayúscula en la contraseña. (Valor predeterminado = true)
- **RequireLowercaseCharacters:** requiere que al menos haya un carácter en minúscula en la contraseña. (Valor predeterminado = true)
- **RequireNumbers:** requiere que al menos haya un número en la contraseña. (Valor predeterminado = true)
- **MinimumPasswordLength:** longitud mínima de la contraseña. (Predeterminado = 7 o más)
- **PasswordReusePrevention:** número de contraseñas antes de que se permita reutilizarlas. (Valor predeterminado = 4)

- **MaxPasswordAge**— Cantidad de días antes de que la contraseña expire. (Valor predeterminado = 90)

 Note

El 30 de mayo de 2025, Security Hub eliminó este control del estándar PCI DSS v4.0.1. La versión 4.0.1 de PCI DSS ahora requiere que las contraseñas tengan un mínimo de 8 caracteres. Este control sigue aplicándose al estándar PCI DSS v3.2.1, que tiene diferentes requisitos de contraseña.

[Para evaluar las políticas de contraseñas de las cuentas con respecto a los requisitos de la versión 4.0.1 de la PCI DSS, puede utilizar el control IAM.7.](#) Este control necesita que las contraseñas tengan 8 caracteres como mínimo. También admite valores personalizados para la longitud de la contraseña y otros parámetros. El control IAM.7 forma parte del estándar PCI DSS v4.0.1 de Security Hub.

Corrección

Para actualizar su política de contraseñas y usar la configuración recomendada, consulte [Establecer una política de contraseñas de cuentas para los usuarios de IAM](#) en la Guía del usuario de IAM.

[IAM.11] Asegurar que la política de contraseñas de IAM requiera al menos una letra mayúscula

Requisitos relacionados: Indicador de referencia de CIS AWS v1.2.0/1.5, NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, NIST.800-171.r2 3.5.8, NIST.800-171.r2 3.5.9, PCI DSS v4.0.1/8.3.6

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS:::Account

Regla de AWS Config : [iam-password-policy](#)

Tipo de programa: Periódico

Parámetros: ninguno

Las políticas de contraseñas aplican, en parte, los requisitos de complejidad de las contraseñas. Utilice las políticas de contraseñas de IAM para garantizar que las contraseñas utilicen diferentes conjuntos de caracteres.

CIS recomienda que la política de contraseñas exija al menos una letra mayúscula. La configuración de una política de complejidad de contraseñas aumenta la resiliencia de la cuenta ante intentos de inicio de sesión por fuerza bruta.

Corrección

Para cambiar la política de contraseñas, consulte [Configurar una política de contraseñas de cuentas para los usuarios de IAM](#) en la Guía del usuario de IAM. Para lograr una Contraseña fuerte, seleccione Se requiere al menos una letra mayúscula del alfabeto latino (A-Z).

[IAM.12] Asegurar que la política de contraseñas de IAM requiera al menos una letra minúscula

Requisitos relacionados: Indicador de referencia de CIS AWS v1.2.0/1.6, NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, NIST.800-171.r2 3.5.8, NIST.800-171.r2 3.5.9, PCI DSS v4.0.1/8.3.6

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS :: Account

Regla de AWS Config : [iam-password-policy](#)

Tipo de programa: Periódico

Parámetros: ninguno

Las políticas de contraseñas aplican, en parte, los requisitos de complejidad de las contraseñas. Utilice las políticas de contraseñas de IAM para garantizar que las contraseñas utilicen diferentes conjuntos de caracteres. CIS recomienda que la política de contraseñas exija al menos una letra minúscula. La configuración de una política de complejidad de contraseñas aumenta la resiliencia de la cuenta ante intentos de inicio de sesión por fuerza bruta.

Corrección

Para cambiar la política de contraseñas, consulte [Configurar una política de contraseñas de cuentas para los usuarios de IAM](#) en la Guía del usuario de IAM. Para lograr una Contraseña fuerte, seleccione Se requiere al menos una letra minúscula del alfabeto latino (A-Z).

[IAM.13] Asegurar que la política de contraseñas de IAM requiera al menos un símbolo

Requisitos relacionados: Indicador de referencia de CIS AWS v1.2.0/1.7, NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, NIST.800-171.r2 3.5.8, NIST.800-171.r2 3.5.9, PCI DSS v4.0.1/8.3.6

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS:::Account

Regla de AWS Config : [iam-password-policy](#)

Tipo de programa: Periódico

Parámetros: ninguno

Las políticas de contraseñas aplican, en parte, los requisitos de complejidad de las contraseñas. Utilice las políticas de contraseñas de IAM para garantizar que las contraseñas utilicen diferentes conjuntos de caracteres.

CIS recomienda que la política de contraseñas exija al menos un símbolo. La configuración de una política de complejidad de contraseñas aumenta la resiliencia de la cuenta ante intentos de inicio de sesión por fuerza bruta.

Corrección

Para cambiar la política de contraseñas, consulte [Configurar una política de contraseñas de cuentas para los usuarios de IAM](#) en la Guía del usuario de IAM. Para la Seguridad de la contraseña, seleccione Requerir al menos un carácter no alfanumérico.

[IAM.14] Asegurar que la política de contraseñas de IAM requiera al menos un número

Requisitos relacionados: Indicador de referencia de CIS AWS v1.2.0/1.8, NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, NIST.800-171.r2 3.5.8, NIST.800-171.r2 3.5.9, PCI DSS v4.0.1/8.3.6

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS:::Account

Regla de AWS Config : [iam-password-policy](#)

Tipo de programa: Periódico

Parámetros: ninguno

Las políticas de contraseñas aplican, en parte, los requisitos de complejidad de las contraseñas. Utilice las políticas de contraseñas de IAM para garantizar que las contraseñas utilicen diferentes conjuntos de caracteres.

CIS recomienda que la política de contraseñas exija al menos un número. La configuración de una política de complejidad de contraseñas aumenta la resiliencia de la cuenta ante intentos de inicio de sesión por fuerza bruta.

Corrección

Para cambiar la política de contraseñas, consulte [Configurar una política de contraseñas de cuentas para los usuarios de IAM](#) en la Guía del usuario de IAM. Para la Seguridad de la contraseña, seleccione Requerir al menos un número.

[IAM.15] Asegurar que la política de contraseñas de IAM requiera una longitud mínima de 14 o más

Requisitos relacionados: Indicador de referencia de CIS AWS v3.0.0/1.8, Indicador de referencia de CIS v1.4.0/1.8, Indicador de referencia de CIS AWS v1.2.0/1.9, NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, AWS NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.9

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS:::Account

Regla de AWS Config : [iam-password-policy](#)

Tipo de programa: Periódico

Parámetros: ninguno

Las políticas de contraseñas aplican, en parte, los requisitos de complejidad de las contraseñas. Utilice las políticas de contraseñas de IAM para garantizar que las contraseñas tengan como mínimo una determinada longitud.

CIS recomienda que la política de contraseñas exija al menos una longitud de contraseña de 14 caracteres. La configuración de una política de complejidad de contraseñas aumenta la resiliencia de la cuenta ante intentos de inicio de sesión por fuerza bruta.

Corrección

Para cambiar la política de contraseñas, consulte [Configurar una política de contraseñas de cuentas para los usuarios de IAM](#) en la Guía del usuario de IAM. Para la Longitud mínima de la contraseña, introduzca **14** o un número mayor.

[IAM.16] Asegurar que la política de contraseñas de IAM impida la reutilización de contraseñas

Requisitos relacionados: Indicador de referencia de CIS AWS v3.0.0/1.9, Indicador de referencia de CIS v1.4.0/1.9, Indicador de referencia de CIS AWS v1.2.0/1.10, NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, AWS NIST.800-171.r2 3.5.8, NIST.800-171.r2 3.5.9, PCI DSS v4.0.1/8.3.7

Categoría: Proteger - Administración de acceso seguro

Gravedad: baja

Tipo de recurso: AWS:::Account

Regla de AWS Config : [iam-password-policy](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el número de contraseñas que se deben recordar está establecido en 24. El control falla si el valor no es 24.

Las políticas de contraseñas de IAM pueden evitar la reutilización de una contraseña determinada por el mismo usuario.

CIS recomienda que la política de contraseñas evite la reutilización de contraseñas. Evitar la reutilización de contraseñas de aumenta la resiliencia de la cuenta frente a intentos de inicio de sesión por fuerza bruta.

Corrección

Para cambiar la política de contraseñas, consulte [Configurar una política de contraseñas de cuentas para los usuarios de IAM](#) en la Guía del usuario de IAM. Para Impedir la reutilización de la contraseña, introduzca **24**.

[IAM.17] Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos

Requisitos relacionados: Indicador de referencia de CIS AWS v1.2.0/1.11, NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, NIST.800-171.r2 3.5.8, NIST.800-171.r2 3.5.9, PCI DSS v4.0.1/8.3.9

Categoría: Proteger - Administración de acceso seguro

Gravedad: baja

Tipo de recurso: AWS : : : Account

Regla de AWS Config : [iam-password-policy](#)

Tipo de programa: Periódico

Parámetros: ninguno

Las políticas de contraseñas de IAM pueden requerir que las contraseñas se roten o que caduquen al cabo de un determinado número de días.

CIS recomienda que la política de contraseñas haga caducar las contraseñas al cabo de 90 días o menos. La reducción de la vida útil de la contraseña aumenta la resiliencia de la cuenta frente a intentos de inicio de sesión por fuerza bruta. Exigir cambios regulares de contraseña también es útil en los siguientes casos:

- Las contraseñas pueden ser robadas o estar en peligro sin que usted lo sepa. Esto puede ocurrir debido a un sistema amenazado, una vulnerabilidad de software o una amenaza interna.
- Algunos filtros web corporativas y gubernamentales o servidores proxy puede interceptar y registrar el tráfico incluso si está cifrado.
- Muchas personas utilizan la misma contraseña para muchos sistemas como, por ejemplo, trabajo, correo electrónico y personal.
- Algunas estaciones de trabajo de usuarios finales en peligro podrían tener un registrador de combinación de teclas.

Corrección

Para cambiar la política de contraseñas, consulte [Configurar una política de contraseñas de cuentas para los usuarios de IAM](#) en la Guía del usuario de IAM. Para Activar la caducidad de la contraseña, introduzca **90** o un número menor.

[IAM.18] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support

Requisitos relacionados: Indicador de referencia de CIS AWS v3.0.0/1.17, Indicador de referencia de CIS v1.4.0/1.17, Indicador de referencia de CIS AWS v1.2.0/1.20, NIST.800-171.r2 3.1.2, PCI AWS DSS v4.0.1/12.10.3

Categoría: Proteger - Administración de acceso seguro

Gravedad: baja

Tipo de recurso: AWS:::Account

Regla de AWS Config : [iam-policy-in-use](#)

Tipo de programa: Periódico

Parámetros:

- policyARN: arn:*partition*:iam::aws:policy/AWSSupportAccess (no personalizable)
- policyUsageType: ANY (no personalizable)

AWS proporciona un centro de soporte que se puede utilizar para la notificación y respuesta a incidentes, así como para brindar soporte técnico y servicios al cliente.

Cree un rol de IAM para permitir que los usuarios autorizados administren incidentes con AWS Support. Al implementar privilegios mínimos para el control de acceso, un rol de IAM requerirá una política de IAM adecuada para permitir el acceso al centro de soporte técnico con el fin de gestionar incidentes con. Soporte

Note

AWS Config debe habilitarse en todas las regiones en las que se utiliza Security Hub. Sin embargo, el registro de recursos globales se puede habilitar en una sola región. Si solo registra recursos globales en una única región, puede desactivar este control en todas las regiones salvo aquella en la que haya registrado los recursos globales.

Corrección

Para solucionar este problema, cree un rol que permita a los usuarios autorizados administrar incidentes de Soporte .

Cómo crear el rol que se utilizará para el Soporte acceso de

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación de IAM, elija Roles y, a continuación, Crear rol.
3. En Tipo de rol, elija Otro Cuenta de AWS.
4. En Account ID, escriba el Cuenta de AWS ID del Cuenta de AWS al que desea conceder acceso a los recursos.

Si los usuarios o grupos que asumirán este rol están en la misma cuenta, introduzca el número de cuenta local.

Note

El administrador de la cuenta especificada puede conceder permiso para asumir este rol a cualquier usuario de en esa cuenta. Para ello, el administrador asocia una política al usuario o grupo que concede permiso para la acción `sts:AssumeRole`. En esa política, el recurso debe ser el ARN del rol.

5. Elija Siguiente: permisos.
6. Busque la política administrada `AWSSupportAccess`.
7. Seleccione la casilla de verificación de la política administrada `AWSSupportAccess`.
8. Elija Siguiente: etiquetas.
9. (Opcional) Para agregar metadatos al rol, asocie etiquetas como pares clave-valor.

Para obtener más información sobre el uso de etiquetas en IAM, consulte [Etiquetado de usuarios y roles de IAM](#) en la Guía del usuario de IAM.

10. Elija Siguiente: Revisar.
11. Escriba un nombre para el rol en Nombre de rol.

Los nombres de rol deben ser únicos en su Cuenta de AWS. No distinguen entre mayúsculas y minúsculas.

12. (Opcional) En Descripción del rol, introduzca una descripción para el nuevo rol.

13. Revise el rol y, a continuación, elija Create role (Crear rol).

[IAM.19] MFA se debe habilitar para todos los usuarios de IAM

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), (1), NIST.800-53.r5 AC-3 (2), (6), NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 (8), NIST.800-53.r5 IA-2 NIST.800-171.r2 3.3.8, NIST.800-53.r5 IA-2 NIST.800-171.r2 3.5.3, NIST.800-171.r2 3.7.5, PCI DSS v3.2.1/8.3.1, PCI DSS v4.0.1/8.4.2

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS::IAM::User

Regla de AWS Config : [iam-user-mfa-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si los usuarios de IAM tienen habilitada la autenticación multifactor (MFA).

Note

AWS Config debe habilitarse en todas las regiones en las que se utiliza Security Hub. Sin embargo, el registro de recursos globales se puede habilitar en una sola región. Si solo registra recursos globales en una única región, puede desactivar este control en todas las regiones salvo aquella en la que haya registrado los recursos globales.

Corrección

Para añadir MFA a los usuarios de IAM, consulte [Habilitar dispositivos de MFA para los usuarios AWS](#) en la Guía del usuario de IAM.

[IAM.20] Evite el uso del usuario raíz

Important

Security Hub retiró este control en abril de 2024. Para obtener más información, consulte [Registro de cambios para los controles CSPM de Security Hub](#).

Requisitos relacionados: Indicador de referencia de de de AWS CIS v1.2.0/1.1

Categoría: Proteger - Administración de acceso seguro

Gravedad: baja

Tipo de recurso: AWS::IAM::User

Regla de AWS Config : use-of-root-account-test (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si una Cuenta de AWS tiene restricciones en cuanto al uso del usuario raíz. El control evalúa los siguientes recursos:

- Temas de Amazon Simple Notification Service (Amazon SNS)
- AWS CloudTrail senderos
- Filtros métricos asociados a las CloudTrail rutas
- CloudWatch Alarmas de Amazon basadas en los filtros

Esta comprobación da como resultado FAILED si una o varias de las siguientes afirmaciones son verdaderas:

- No hay CloudTrail rutas en la cuenta.
- La CloudTrail ruta está habilitada, pero no configurada con al menos una ruta multirregional que incluya eventos de administración de lectura y escritura.
- La CloudTrail ruta está habilitada, pero no está asociada a un grupo de CloudWatch registros de registros de.
- No se utiliza el filtro métrico exacto prescrito por el Center for Internet Security (CIS). El filtro métrico prescrito es '`{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent"}`'.
- No hay CloudWatch alarmas basadas en el filtro de métricas en la cuenta.
- CloudWatch las alarmas configuradas para enviar notificaciones al tema de SNS asociado no se activan en función del estado de la alarma.

- El tema de SNS no cumple con las [restricciones para enviar un mensaje a un tema de SNS](#).
- El tema de SNS no tiene al menos un suscriptor.

Esta comprobación da como resultado NO_DATA si una o más de las siguientes afirmaciones son verdaderas:

- Una ruta multirregional se basa en una Región diferente. Security Hub solo puede generar resultados en la Región en la que se encuentra el rastro.
- Una ruta multirregional pertenece a una cuenta diferente. Security Hub solo puede generar resultados para la cuenta propietaria de la ruta.

Esta comprobación da como resultado WARNING si una o más de las siguientes afirmaciones son verdaderas:

- La cuenta corriente no es propietaria del tema de SNS al que se hace referencia en la CloudWatch alarma.
- La cuenta actual no tiene acceso al tema de SNS al invocar la API de SNS de `ListSubscriptionsByTopic`.

Note

Recomendamos utilizar los registros de la organización para registrar los eventos de varias cuentas de una organización. Las rutas de organización son rutas multirregionales de forma predeterminada y solo las puede gestionar la cuenta AWS Organizations de administración de o la cuenta de administrador CloudTrail delegado. El uso de un registro de la organización da como resultado un estado de control de NO_DATA para los controles evaluados en las cuentas de los miembros de la organización. En las cuentas de los miembros, Security Hub solo genera resultados para los recursos propiedad de los miembros. Los resultados relacionados con los registros de la organización se generan en la cuenta del propietario del recurso. Puede ver estos resultados en su cuenta de administrador delegado de Security Hub mediante la agregación entre regiones.

Como práctica recomendada, utilice sus credenciales de usuario raíz solo cuando sea necesario para [realizar tareas de administración de cuentas y servicios](#). Aplique políticas de IAM directamente a los grupos y roles, pero no a los usuarios. Para ver las instrucciones sobre cómo configurar un

administrador para el uso diario, consulte [Creación del primer grupo y usuario administrador de IAM](#) en la Guía de usuario de IAM.

Corrección

Los pasos para solucionar este asunto incluyen configurar un tema de Amazon SNS, CloudTrail un filtro de métricas y una alarma para el filtro de métricas.

Para crear un tema de Amazon SNS

1. [Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/ la v3/home](https://console.aws.amazon.com/sns/la/v3/home).
2. Cree un tema de Amazon SNS que reciba todas las alarmas de CIS.

Cree al menos un suscriptor al tema. Para obtener más información, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

Luego, configure una activa CloudTrail que se aplique a todas las regiones. Para ello, siga los pasos de corrección en [the section called “\[CloudTrail.1\] CloudTrail debe habilitarse y configurarse con al menos un registro de seguimiento para varias regiones que incluya eventos de administración de lectura y escritura”](#).

Anote el nombre del grupo de CloudWatch registros de registros de registros de registros de registros de registros CloudTrail de. Cree el filtro de métricas en el grupo de registro.

Por último, cree el filtro métrico y la alarma.

Para crear un filtro de métricas y alarma

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, seleccione Grupos de registro.
3. Seleccione la casilla de verificación del grupo de CloudWatch registros de registros asociado a la CloudTrail ruta que creó.
4. En Acciones, elija Crear filtro de métricas.
5. En Definir patrón, haga lo siguiente:
 - a. Copie el siguiente patrón y, a continuación, péguelo en el campo Filter Pattern (Patrón de filtros).


```
{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent"}
```

- b. Elija Siguiente.
6. En Asignar métrica, haga lo siguiente:
 - a. En Nombre de filtro, escriba un nombre para el filtro de métricas.
 - b. En Espacio de nombres de métrica, escriba **LogMetrics**.

Si usa el mismo espacio de nombres para todos los filtros de métricas de registro de CIS, todas las métricas de CIS Benchmark se agrupan.
 - c. Para Nombre de métrica, ingrese un nombre para la métrica. Recuerde el nombre de la métrica. Deberá seleccionar la métrica al crear la alarma.
 - d. En Metric Value (Valor de métrica), ingrese **1**.
 - e. Elija Siguiente.
7. En Revisar y crear, compruebe la información que proporcionó para el nuevo filtro de métricas. A continuación, elija Crear filtro de métrica.
8. En el panel de navegación, elija Grupos de registros y, a continuación, elija el filtro que creó en Filtros métricos.
9. Seleccione la casilla de verificación del filtro. Elija Crear alarma.
10. En Especificar métrica y condiciones, realice lo siguiente:
 - a. En Condiciones, vaya a Tipo de umbral y escriba Estático.
 - b. En Definir la condición de alarma, elija Mayor/Igual.
 - c. En Definir el valor umbral, introduzca **1**.
 - d. Elija Siguiente.
11. En Configuración de acciones, haga lo siguiente:
 - a. Para Desencadenador de estado de alarma, elija En alarma.
 - b. En Select an SNS topic, elija Select an existing SNS topic.
 - c. En Enviar notificación a, introduzca el nombre del tema de SNS que creó en el procedimiento anterior.
 - d. Elija Siguiente.

12. En Añadir una descripción, escriba un nombre y la descripción de la alarma, como **CIS-1.1-RootAccountUsage**. A continuación, elija Siguiente.
13. En Vista previa y creación, revise la configuración de la alarma. A continuación, elija Create Alarm (Crear alarma).

[IAM.21] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios

Requisitos relacionados: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), (15), (7),, (10)
NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (2), NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6
(3), NIST.800-171.r2 3.1.1 NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6
NIST.800-171.r2 3.1.2, NIST.800-53.r5 AC-6 NIST.800-171.r2 3.1.5, NIST.800-171.r2 3.1.7,
NIST.800-171.r2 3.3.8, NIST.800-171.r2 3.3.8, NIST.800-171.r2 3.3.9, NIST.800-171.r2 3.13.3,
NIST.800-171.r2 3.13.4

Categoría: Detectar > Gestión de acceso seguro

Gravedad: baja

Tipo de recurso: AWS::IAM::Policy

Regla de AWS Config : [iam-policy-no-statements-with-full-access](#)

Tipo de horario: provocado por un cambio

Parámetros:

- `excludePermissionBoundaryPolicy`: True (no personalizable)

Este control comprueba si las políticas de IAM basadas en la identidad que cree incluyen instrucciones de permiso que utilizan el comodín * para conceder permisos para todas las acciones de cualquier servicio. El control falla si alguna declaración de política incluye "Effect": "Allow" con "Action": "Service:*".

Por ejemplo, la siguiente afirmación de una política da como resultado una conclusión fallida.

```
"Statement": [  
  {  
    "Sid": "EC2-Wildcard",
```

```
"Effect": "Allow",  
"Action": "ec2:*",  
"Resource": "*" } }
```

El control también falla si se usa "Effect": "Allow" con "NotAction": "*service*:*". En ese caso, el NotAction elemento proporciona acceso a todas las acciones en Servicio de AWS, salvo las acciones especificadas enNotAction.

Este control solo se aplica a las políticas de IAM administradas por el cliente. No se aplica a las políticas de IAM gestionadas por AWS.

Cuando se pueden asignar permisos a Servicios de AWS, es importante incluir en sus políticas de IAM las acciones de IAM permitidas de IAM. Debe restringir las acciones de IAM solo a las acciones que sean necesarias. Esto le ayuda a proporcionar permisos con privilegios mínimos. Las políticas demasiado permisivas pueden provocar una escalada de privilegios si las políticas están vinculadas a un director de IAM que podría no requerir el permiso.

En algunos casos, es posible que desee permitir acciones de IAM que tienen un prefijo similar, como DescribeFlowLogs y DescribeAvailabilityZones. En estos casos autorizados, puede añadir un comodín con sufijo al prefijo común. Por ejemplo, ec2:Describe*.

Este control se activa si utiliza una acción de IAM con un prefijo con un comodín con sufijo. Por ejemplo, la siguiente declaración de una política da como resultado que se aprueba una conclusión.

```
"Statement": [  
{  
  "Sid": "EC2-Wildcard",  
  "Effect": "Allow",  
  "Action": "ec2:Describe*",  
  "Resource": "*" }  
]
```

Si agrupa las acciones de IAM relacionadas de esta manera, también puede evitar superar los límites de tamaño de las políticas de IAM.

Note

AWS Config debe habilitarse en todas las regiones en las que se utiliza Security Hub. Sin embargo, el registro de recursos globales se puede habilitar en una sola región. Si solo

registra recursos globales en una única región, puede desactivar este control en todas las regiones salvo aquella en la que haya registrado los recursos globales.

Corrección

Para solucionar este problema, actualice sus políticas de IAM para que no permitan todos los privilegios administrativos “*”. Para conocer los detalles acerca de cómo editar una política de IAM, consulte [Edición de políticas de IAM](#) en la Guía del usuario de IAM.

[IAM.22] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días

Requisitos relacionados: Indicador de referencia de CIS AWS v3.0.0/1.12, Indicador de referencia de CIS v1.4.0/1.12, NIST.800-171.r2 AWS 3.1.2

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS : : IAM : : User

AWS Config regla: [iam-user-unused-credentials-check](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si los usuarios de IAM tienen contraseñas o claves de acceso activas que no se han utilizado durante 45 días o más. Para ello, comprueba si el `maxCredentialUsageAge` parámetro de la AWS Config regla de es igual o superior a 45.

Los usuarios de pueden acceder a AWS los recursos de utilizando diferentes tipos de credenciales, como contraseñas o claves de acceso.

CIS recomienda que elimine o desactive todas las credenciales que han dejado de utilizarse durante 45 días o más. Al deshabilitar o eliminar credenciales innecesarias se reduce la oportunidad de que se utilicen credenciales asociadas a una cuenta en peligro o abandonada.

La AWS Config regla para este control utiliza las operaciones [GetCredentialReport](#) y la [GenerateCredentialReport](#) API, que solo se actualizan cada cuatro horas. Los cambios en los usuarios de IAM pueden tardar hasta cuatro horas en ser visibles para este control.

 Note

AWS Config debe habilitarse en todas las regiones en las que se utiliza Security Hub. Sin embargo, puede habilitar el registro de los recursos globales en una sola región. Si solo registra recursos globales en una única región, puede desactivar este control en todas las regiones salvo aquella en la que haya registrado los recursos globales.

Corrección

Al ver la información del usuario en la consola de IAM, hay columnas para la antigüedad de la clave de acceso, la antigüedad de la Contraseña y la Última actividad. Si el valor en cualquiera de estas columnas es superior a 45 días, desactive las credenciales de esos usuarios.

También puede utilizar los [informes de credenciales](#) para monitorizar a los usuarios e identificar a aquellos que no tienen actividad durante 45 días o más. Puede descargar los informes de credenciales en formato .csv desde la consola de IAM.

Después de identificar las cuentas inactivas o las credenciales no utilizadas, desactívalas. Para obtener instrucciones, consulte [Creación, cambio o eliminación de la contraseña de un usuario de IAM \(consola\)](#) en la Guía del usuario de IAM.

[IAM.23] Los analizadores del Analizador de acceso de IAM deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::AccessAnalyzer::Analyzer`

AWS Config Regla de: `tagged-accessanalyzer-analyzer` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un analizador administrado por AWS Identity and Access Management Access Analyzer (Analizador de acceso de IAM Access Analyzer) tiene etiquetas con las claves específicas definidas en el parámetro. `requiredTagKeys` El control lanza error si el analizador no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el analizador no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un analizador, consulte [TagResource](#) en la Referencia de la API del Analizador de acceso de AWS IAM.

[IAM.24] Los roles de IAM deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IAM::Role

AWS Config Regla de: tagged-iam-role (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un rol de AWS Identity and Access Management (IAM) tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el rol no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el rol no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un rol de IAM, consulte [Etiquetado de recursos de IAM](#) en la Guía del usuario de IAM.

[IAM.25] Los usuarios de IAM deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IAM::User

AWS Config Regla de: tagged-iam-user (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un usuario de AWS Identity and Access Management (IAM) tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el usuario no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el usuario no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones

cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un usuario de IAM, consulte [Etiquetado de recursos de IAM](#) en la Guía del usuario de IAM.

[IAM.26] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse

Requisitos relacionados: Indicador de referencia de de de CIS AWS v3.0.0/1.19

Categoría: Identificar > Cumplimiento

Gravedad: media

Tipo de recurso: AWS::IAM::ServerCertificate

AWS Config regla: [iam-server-certificate-expiration-check](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un certificado de SSL/TLS server certificate that is managed in IAM has expired. The control fails if the expired SSL/TLS servidor activo no se elimina.

Para habilitar las conexiones HTTPS en su sitio web o aplicación en AWS, necesita un certificado de servidor SSL/TLS. Puede utilizar IAM o AWS Certificate Manager (ACM) para almacenar e implementar certificados de servidor. Utilice IAM como Certificate Manager solo cuando deba admitir conexiones HTTPS en una Región de AWS que no es compatible con ACM. IAM cifra de forma segura sus claves privadas y almacena la versión cifrada en el almacenamiento de certificados SSL

de IAM. IAM admite la implementación de certificados de servidor en todas las regiones, pero debe obtener su certificado de un proveedor externo para utilizarlo con AWS. No se puede cargar un certificado de ACM en IAM. Además, no se puede administrar los certificados desde la consola de IAM. Cuando elimina los certificados SSL/TLS vencidos, se elimina el riesgo de que un certificado no válido se implemente por accidente en un recurso, lo que puede dañar la credibilidad de la aplicación o el sitio web subyacentes.

Corrección

Para eliminar un certificado de servidor de IAM, consulte [Administración de los certificados de servidor en IAM](#) en la Guía del usuario de IAM.

[IAM.27] Las identidades de IAM no deben tener adjunta la política AWSCloudShellFullAccess

Requisitos relacionados: Indicador de referencia de de de CIS AWS v3.0.0/1.22

Categoría: Proteger > Administración de acceso seguro > Políticas de IAM seguras

Gravedad: media

Tipo de recurso: AWS::IAM::Role, AWS::IAM::User, AWS::IAM::Group

AWS Config regla: [iam-policy-blacklisted-check](#)

Tipo de horario: provocado por un cambio

Parámetros:

- «PolicyArns»: «arn:aws:iam::aws:» policy/AWSCloudShellFullAccess,arn:aws-cn:iam::aws:policy/AWSCloudShellFullAccess, arn:aws-us-gov:iam::aws:policy/AWSCloudShellFullAccess

Este control comprueba si una identidad de IAM (usuario, rol o grupo) tiene la política AWS administrada AWSCloudShellFullAccess adjunta. El control lanza error si una identidad de IAM tiene la política AWSCloudShellFullAccess adjunta.

AWS CloudShell permite ejecutar de manera práctica comandos de la CLI en los Servicios de AWS. La política AWS administrada AWSCloudShellFullAccess proporciona acceso completo a CloudShell, lo que permite cargar y descargar archivos entre el sistema local del usuario y el

CloudShell entorno. En el CloudShell entorno, un usuario tiene permisos sudo y puede acceder a Internet. Como resultado, cuando se adjunta esta política administrada a una identidad de IAM, los usuarios pueden instalar software de transferencia de archivos y mover datos de CloudShell a servidores de Internet externos. Recomendamos seguir el principio de privilegio mínimo y adjuntar permisos más limitados a las identidades de IAM.

Corrección

Para desasociar la política `AWSCloudShellFullAccess` de una identidad de IAM, consulte [Cómo agregar y eliminar permisos de identidad de IAM](#) en la Guía del usuario de IAM.

[IAM.28] El analizador de acceso externo del Analizador de acceso de IAM debe habilitarse

Requisitos relacionados: Indicador de referencia de de de CIS AWS v3.0.0/1.20

Categoría: Detectar > Servicios de detección > Supervisión de uso con privilegios

Gravedad: alta

Tipo de recurso: `AWS::AccessAnalyzer::Analyzer`

AWS Config regla: [iam-external-access-analyzer-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si una Cuenta de AWS tiene habilitado un analizador de acceso externo de IAM Access Analyzer. El control lanza error si la cuenta no tiene un analizador de acceso externo habilitado en la Región de AWS seleccionada.

Los analizadores de acceso externo del Analizador de acceso de IAM Access Analyzer ayudan a identificar recursos, como los buckets de Amazon Simple Storage Service (Amazon S3) o los roles de IAM IAM, que se comparten con una entidad externa. De esta manera, se evita el acceso no deseado a los recursos y los datos. El Analizador de acceso de IAM es regional y debe estar habilitado en cada región. Para identificar recursos compartidos con entidades principales externas, un analizador de acceso utiliza un razonamiento lógico para analizar las políticas basadas en recursos en su entorno. AWS Cuando crea un analizador de acceso externo, puede crearlo y habilitarlo para toda la organización o las cuentas individuales.

 Note

Si una cuenta forma parte de una organización AWS Organizations, este control no tiene en cuenta los analizadores de acceso externos que especifican la organización como zona de confianza y están habilitados para la organización de la región actual. Si su organización usa este tipo de configuración, considere deshabilitar este control para las cuentas de los miembros individuales de su organización en la región.

Corrección

Para obtener información sobre cómo habilitar un analizador de acceso externo en una región específica, consulte [Primeros pasos con IAM Access Analyzer](#) en la Guía del usuario de IAM IAM. Debe habilitar un analizador en cada región en la que desee supervisar el acceso a sus recursos.

Controles de Security Hub para Amazon Inspector

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon Inspector.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Inspector.1] El EC2 escaneo de Amazon Inspector debe estar activado

Requisitos relacionados: PCI DSS v4.0.1/11.3.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: AWS :: Account

Regla de AWS Config : [inspector-ec2-scan-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el EC2 escaneo de Amazon Inspector está activado. En el caso de una cuenta independiente, el control falla si el EC2 escaneo de Amazon Inspector está desactivado en la

cuenta. En un entorno con varias cuentas, el control falla si la cuenta de administrador de Amazon Inspector delegada y todas las cuentas de los miembros no tienen habilitada la EC2 digitalización.

En un entorno con varias cuentas, el control genera resultados solo en la cuenta de administrador delegado de Amazon Inspector. Solo el administrador delegado puede activar o desactivar la función de EC2 escaneo de las cuentas de los miembros de la organización. Los miembros de Amazon Inspector no pueden modificar esta configuración desde sus cuentas. Este control genera FAILED resultados si el administrador delegado tiene una cuenta de miembro suspendida que no tiene habilitada la EC2 digitalización de Amazon Inspector. Para recibir un resultado PASSED, el administrador delegado debe desvincular estas cuentas suspendidas en Amazon Inspector.

El EC2 escaneo de Amazon Inspector extrae los metadatos de su instancia de Amazon Elastic Compute Cloud (Amazon EC2) y, a continuación, los compara con las reglas recopiladas en los avisos de seguridad para obtener resultados. Amazon Inspector analiza las instancias en busca de vulnerabilidades en los paquetes y problemas de accesibilidad a la red. Para obtener información sobre los sistemas operativos compatibles, incluido el sistema operativo que se puede escanear sin un agente SSM, consulte [Sistemas operativos compatibles: EC2 digitalización de Amazon](#).

Corrección

Para activar el EC2 escaneo de Amazon Inspector, consulte [Activación de escaneos](#) en la Guía del usuario de Amazon Inspector.

[Inspector.2] El análisis de ECR en Amazon Inspector debe estar habilitado

Requisitos relacionados: PCI DSS v4.0.1/11.3.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: AWS :: Account

Regla de AWS Config : [inspector-ecr-scan-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si está habilitado el análisis de ECR en Amazon Inspector. En el caso de una cuenta independiente, el control lanza un error si el análisis de ECR en Amazon Inspector está

desactivado en la cuenta. En un entorno con varias cuentas, el control lanza un error si ni la cuenta de administrador delegado de Amazon Inspector ni ninguna de las cuentas de los miembros tienen habilitado el análisis de ECR.

En un entorno con varias cuentas, el control genera resultados solo en la cuenta de administrador delegado de Amazon Inspector. Solo el administrador delegado puede activar o desactivar la característica de análisis de ECR para las cuentas de los miembros en la organización. Los miembros de Amazon Inspector no pueden modificar esta configuración desde sus cuentas. Este control genera resultados FAILED si el administrador delegado tiene una cuenta de miembro suspendida que no tiene habilitado el análisis de ECR en Amazon Inspector. Para recibir un resultado PASSED, el administrador delegado debe desvincular estas cuentas suspendidas en Amazon Inspector.

Amazon Inspector analiza las imágenes de contenedores almacenadas en Amazon Elastic Container Registry (Amazon ECR) en busca de vulnerabilidades en el software para generar resultados de vulnerabilidades de paquetes. Al activar los análisis de Amazon Inspector para Amazon ECR, se configura Amazon Inspector como servicio de análisis preferido para su registro privado. Amazon Inspector reemplaza los análisis básicos, que se ofrecen de forma gratuita en Amazon ECR, por análisis mejorados, que se ofrecen y facturan a través de Amazon Inspector. Los análisis mejorados le ofrecen la ventaja de analizar vulnerabilidades tanto de sistemas operativos como de paquetes de lenguajes de programación en el nivel de registro. Puede revisar los resultados descubiertos a partir de análisis mejorados en el nivel de imagen, para cada capa de la imagen, en la consola de Amazon ECR. Además, puedes revisar estos resultados y trabajar con ellos en otros servicios que no están disponibles para los resultados de digitalización básicos, como AWS Security Hub Amazon EventBridge.

Corrección

Para habilitar el análisis de ECR en Amazon Inspector, consulte [Activating scans](#) en la Guía del usuario de Amazon Inspector.

[Inspector.3] El análisis de código de Lambda en Amazon Inspector debe estar habilitado

Requisitos relacionados: PCI DSS v4.0.1/6.2.4, PCI DSS v4.0.1/6.3.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: AWS:::Account

Regla de AWS Config : [inspector-lambda-code-scan-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si está habilitado el análisis de código de Lambda en Amazon Inspector. En el caso de una cuenta independiente, el control lanza un error si el análisis de código de Lambda en Amazon Inspector está desactivado en la cuenta. En un entorno de varias cuentas, el control lanza un error si ni la cuenta de administrador delegado de Amazon Inspector ni ninguna de las cuentas de los miembros tienen habilitado el análisis de código de Lambda.

En un entorno con varias cuentas, el control genera resultados solo en la cuenta de administrador delegado de Amazon Inspector. Solo el administrador delegado puede activar o desactivar la característica de análisis de código de Lambda para las cuentas de los miembros en la organización. Los miembros de Amazon Inspector no pueden modificar esta configuración desde sus cuentas. Este control genera resultados FAILED si el administrador delegado tiene una cuenta de miembro suspendida que no tiene habilitado el análisis de códigos de Lambda en Amazon Inspector. Para recibir un resultado PASSED, el administrador delegado debe desvincular estas cuentas suspendidas en Amazon Inspector.

El escaneo de código Lambda de Amazon Inspector analiza el código de la aplicación personalizada dentro de una AWS Lambda función para detectar vulnerabilidades en el código según las prácticas recomendadas AWS de seguridad. El análisis de código de Lambda puede detectar fallos de inyección, fugas de datos, errores de criptografía débil o una falta de cifrado en el código. Esta función [Regiones de AWS solo está disponible de forma específica](#). Puede activar el análisis de código de Lambda junto al análisis estándar de Lambda (consulte [\[Inspector.4\] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado](#)).

Corrección

Para habilitar el análisis de código de Lambda en Amazon Inspector, consulte [Activación de análisis](#) en la Guía del usuario de Amazon Inspector.

[Inspector.4] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado

Requisitos relacionados: PCI DSS v4.0.1/6.2.4, PCI DSS v4.0.1/6.3.1

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: AWS:::Account

Regla de AWS Config : [inspector-lambda-standard-scan-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si está habilitado el análisis estándar de Lambda en Amazon Inspector. En el caso de una cuenta independiente, el control lanza un error si el análisis estándar de Lambda en Amazon Inspector está desactivado en la cuenta. En un entorno de varias cuentas, el control lanza un error si ni la cuenta de administrador delegado de Amazon Inspector ni ninguna de las cuentas de los miembros tienen habilitado el análisis estándar de Lambda.

En un entorno con varias cuentas, el control genera resultados solo en la cuenta de administrador delegado de Amazon Inspector. Solo el administrador delegado puede activar o desactivar la característica de análisis estándar de Lambda para las cuentas de los miembros en la organización. Los miembros de Amazon Inspector no pueden modificar esta configuración desde sus cuentas. Este control genera resultados FAILED si el administrador delegado tiene una cuenta de miembro suspendida que no tiene habilitado el análisis estándar de Lambda en Amazon Inspector. Para recibir un resultado PASSED, el administrador delegado debe desvincular estas cuentas suspendidas en Amazon Inspector.

El escaneo estándar de Amazon Inspector Lambda identifica las vulnerabilidades de software en las dependencias del paquete de aplicaciones que añada al código y las capas de AWS Lambda función. Si Amazon Inspector detecta una vulnerabilidad en las dependencias del paquete de la aplicación de la función de Lambda, Amazon Inspector genera un resultado detallado del tipo Package Vulnerability. Puede activar el análisis de código de Lambda junto al análisis estándar de Lambda (consulte [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)).

Corrección

Para habilitar el análisis estándar de Lambda en Amazon Inspector, consulte [Activación de análisis](#) en la Guía del usuario de Amazon Inspector.

Controles de Security Hub para AWS IoT

Estos AWS Security Hub controles evalúan el AWS IoT servicio y los recursos.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

Los perfiles de AWS IoT Device Defender seguridad [IoT.1] deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoT::SecurityProfile`

Regla de AWS Config : `tagged-iot-securityprofile` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un perfil de AWS IoT Device Defender seguridad tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el perfil de seguridad no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el perfil de seguridad no

está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un perfil AWS IoT Device Defender de seguridad, consulte [Etiquetar AWS IoT los recursos](#) en la AWS IoT Guía para desarrolladores.

[IoT.2] las acciones de AWS IoT Core mitigación deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoT::MitigationAction`

Regla de AWS Config : `tagged-iot-mitigationaction` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si una acción de AWS IoT Core mitigación tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la acción de mitigación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la acción de mitigación no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre

ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una acción de AWS IoT Core mitigación, consulta Cómo [etiquetar tus AWS IoT recursos](#) en la AWS IoT Guía para desarrolladores.

AWS IoT Core Las dimensiones de [IoT.3] deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IoT::Dimension

Regla de AWS Config : tagged-iot-dimension (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si una AWS IoT Core dimensión tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la dimensión no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la dimensión no está etiquetada

con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una AWS IoT Core dimensión, consulta Cómo [etiquetar tus AWS IoT recursos](#) en la AWS IoT Guía para desarrolladores.

Los AWS IoT Core autorizadores [IoT.4] deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoT::Authorizer`

Regla de AWS Config : `tagged-iot-authorizer` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un AWS IoT Core autorizador tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el autorizador no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el autorizador no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre

ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un AWS IoT Core autorizador, consulta Cómo [etiquetar tus AWS IoT recursos](#) en la Guía para desarrolladores.AWS IoT

Los alias de los AWS IoT Core roles [IoT.5] deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IoT::RoleAlias

Regla de AWS Config : tagged-iot-rolealias (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si el alias de un AWS IoT Core rol tiene etiquetas con las claves específicas definidas en el parámetrorequiredTagKeys. El control lanza un error si el alias de un rol no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro requiredTagKeys. Si no se proporciona el parámetro requiredTagKeys, el control solo

comprueba la existencia de una clave de etiqueta y lanza un error si el alias de un rol no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un alias de AWS IoT Core rol, consulta Cómo [etiquetar tus AWS IoT recursos](#) en la AWS IoT Guía para desarrolladores.

AWS IoT Core Las políticas [IoT.6] deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoT::Policy`

Regla de AWS Config : `tagged-iot-policy` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si una AWS IoT Core política tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la política no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la política no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre

ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una AWS IoT Core política, consulta Cómo [etiquetar tus AWS IoT recursos](#) en la AWS IoT Guía para desarrolladores.

Controles de Security Hub para eventos de AWS IoT

Estos AWS Security Hub controles evalúan el servicio y los recursos de AWS IoT Events.

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[IoTEvents .1] Las entradas de AWS IoT Events deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IoTEvents::Input

Regla de AWS Config : iotevents-input-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una entrada de AWS IoT Events tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si la entrada no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si la entrada no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una entrada de AWS IoT Events, consulta Cómo [etiquetar tus AWS IoT Events recursos](#) en la Guía para AWS IoT Events desarrolladores.

[IoTEvents .2] Los modelos de detectores de AWS IoT Events deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoTEvents::DetectorModel`

Regla de AWS Config : `iotevents-detector-model-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un modelo de detector de AWS IoT Events tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el modelo de detector no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el modelo de detector no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para

sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas, AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un modelo de detector de eventos de AWS IoT, consulta Cómo [etiquetar tus AWS IoT Events recursos](#) en la Guía para AWS IoT Events desarrolladores.

[Io TEvents .3] Los modelos de alarma de AWS IoT Events deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoTEvents::AlarmModel`

Regla de AWS Config : `iotevents-alarm-model-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.		que cumplan con AWS los requisitos .	

Este control comprueba si un modelo de alarma de AWS IoT Events tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el modelo de alarma no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el modelo de alarma no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws :`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado,

consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un modelo de alarma de AWS IoT Events, consulta Cómo [etiquetar tus AWS IoT Events recursos](#) en la Guía para AWS IoT Events desarrolladores.

Controles de Security Hub para AWS IoT SiteWise

Estos AWS Security Hub controles evalúan el SiteWise servicio y los recursos de AWS IoT.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[IoT SiteWise.1] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoTSiteWise::AssetModel`

Regla de AWS Config: `iotsitewise-asset-model-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	de etiqueta distinguen entre mayúsculas y minúsculas.		con AWS los requisitos .	

Este control comprueba si un modelo de SiteWise activos de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el modelo de activos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el modelo de activos no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas, AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un modelo de SiteWise activos de AWS IoT, consulte [Etiquete sus AWS IoT SiteWise recursos](#) en la Guía del AWS IoT SiteWise usuario.

[IoT SiteWise.2] SiteWise Los paneles de AWS IoT deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IoTSiteWise::Dashboard

Regla de AWS Config: iotsitewise-dashboard-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un SiteWise panel de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el panel no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el panel no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno

u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas, AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un SiteWise panel de AWS IoT, consulta Cómo [etiquetar tus AWS IoT SiteWise recursos](#) en la Guía del AWS IoT SiteWise usuario.

[IoT SiteWise.3] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IoTSiteWise::Gateway

Regla de AWS Config: iotsitewise-gateway-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una SiteWise pasarela de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si la puerta de enlace no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si la puerta de enlace no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para agregar etiquetas a una SiteWise puerta de enlace de AWS IoT, consulte [Etiquete sus AWS IoT SiteWise recursos](#) en la Guía del AWS IoT SiteWise usuario.

[IoT Site Wise.4] Los SiteWise portales de AWS IoT deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IoTSiteWise::Portal

Regla de AWS Config : iotsitewise-portal-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un SiteWise portal de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el portal no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y produce un error si el portal no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas, AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un SiteWise portal de AWS IoT, consulte [Etiquete sus AWS IoT SiteWise recursos](#) en la Guía del AWS IoT SiteWise usuario.

[IoT Site Wise.5] Los SiteWise proyectos de AWS IoT deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoTSiteWise::Project`

Regla de AWS Config: `iotsitewise-project-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un SiteWise proyecto de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el proyecto no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el proyecto no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un SiteWise proyecto de AWS IoT, consulte [Etiquetar sus AWS IoT SiteWise recursos](#) en la Guía del AWS IoT SiteWise usuario.

Controles de Security Hub para AWS IoT TwinMaker

Estos AWS Security Hub controles evalúan el TwinMaker servicio y los recursos de AWS IoT.

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[IoT Twin Maker.1] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IoT::TwinMaker::SyncJob

Regla de AWS Config: iottwinmaker-sync-job-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un trabajo de TwinMaker sincronización de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el trabajo de sincronización no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y produce un error si el trabajo de sincronización no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws :`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un trabajo de TwinMaker sincronización de AWS IoT, consulte [TagResource](#) en la Guía del usuario de AWS IoT TwinMaker .

[IoT Twin Maker.2] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IoT::TwinMaker::Workspace

Regla de AWS Config : iottwinmaker-workspace-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un TwinMaker espacio de trabajo de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el espacio de trabajo no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y produce un error si el espacio de trabajo no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas, AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un espacio de TwinMaker trabajo de AWS IoT, consulte [TagResource](#) en la Guía del usuario de AWS IoT TwinMaker .

[IoT Twin Maker.3] TwinMaker Las escenas de AWS IoT deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoT::TwinMaker::Scene`

Regla de AWS Config: `iottwinmaker-scene-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una TwinMaker escena de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si la escena no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si la escena no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para

sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas, AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una TwinMaker escena de AWS IoT, consulte [TagResource](#) en la Guía del usuario de AWS IoT TwinMaker .

[IoT Twin Maker.4] TwinMaker Las entidades de AWS IoT deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IoT::TwinMaker::Entity

Regla de AWS Config : iottwinmaker-entity-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.		que cumplan con AWS los requisitos .	

Este control comprueba si una TwinMaker entidad de AWS IoT tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si la entidad no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si la entidad no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado,

consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para agregar etiquetas a una TwinMaker entidad de AWS IoT, consulte [TagResource](#) en la Guía del usuario de AWS IoT TwinMaker .

Controles de Security Hub para AWS IoT Wireless

Estos AWS Security Hub controles evalúan el servicio y los recursos de AWS IoT Wireless.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[IoTWireless .1] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IoTWireless::MulticastGroup

Regla de AWS Config: iotwireless-multicast-group-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	de etiqueta distinguen entre mayúsculas y minúsculas.		con AWS los requisitos .	

Este control comprueba si un grupo de multidifusión de AWS IoT Wireless tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el grupo de multidifusión no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro. `requiredKeyTags` Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y produce un error si el grupo de multidifusión no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas, AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para agregar etiquetas a un grupo de multidifusión de AWS IoT Wireless, consulte [Etiquetar sus AWS IoT Wireless recursos en la Guía para AWS IoT Wireless](#) desarrolladores.

[IoTWireless .2] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IoTWireless::ServiceProfile

Regla de AWS Config: iotwireless-service-profile-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un perfil de servicio AWS IoT Wireless tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el perfil de servicio no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el perfil de servicio no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un perfil de servicio de AWS IoT Wireless, consulte [Etiquetar sus AWS IoT Wireless recursos](#) en la Guía para AWS IoT Wireless desarrolladores.

[IoT Wireless .3] Las tareas de AWS IoT FUOTA deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IoTWireless::FuotaTask

Regla de AWS Config : iotwireless-fuota-task-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una tarea de actualización del firmware de AWS IoT Wireless over-the-air (FUOTA) tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si la tarea FUOTA no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro. `requiredKeyTags` Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si la tarea FUOTA no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una tarea FUOTA de AWS IoT Wireless, consulta Cómo [etiquetar tus AWS IoT Wireless recursos en la Guía para AWS IoT Wireless](#) desarrolladores.

Controles de Security Hub para Amazon IVS

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon Interactive Video Service (IVS).

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[IVS.1] Los pares de teclas de reproducción del IVS deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IVS::PlaybackKeyPair`

Regla de AWS Config : `ivs-playback-key-pair-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un par de claves de reproducción de Amazon IVS tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el par de claves de reproducción no tiene ninguna tecla de etiqueta o si no tiene todas las teclas especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el par de claves de reproducción no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un par de claves de reproducción IVS, consulte [TagResource](#) en la referencia de la API de streaming en tiempo real de Amazon IVS.

[IVS.2] Las configuraciones de grabación del IVS deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IVS::RecordingConfiguration

Regla de AWS Config: ivs-recording configuration-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una configuración de grabación de Amazon IVS tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si la configuración de grabación no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si la configuración de grabación no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas, AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una configuración de grabación de IVS, consulte [TagResource](#) en la referencia de la API de streaming en tiempo real de Amazon IVS.

[IVS.3] Los canales de IVS deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IVS::Channel

Regla de AWS Config : `ivs-channel-tagged`

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un canal de Amazon IVS tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control falla si el canal no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el canal no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para

sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un canal de IVS, consulte [TagResource](#) en la referencia de la API de streaming en tiempo real de Amazon IVS.

Controles de Security Hub para Amazon Keyspaces

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon Keyspaces.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Keyspaces.1] Los espacios clave de Amazon Keyspaces deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Cassandra::Keyspace

Regla de AWS Config : cassandra-keyspace-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un espacio de claves de Amazon Keyspaces tiene etiquetas con las claves específicas definidas en el parámetro. `requiredKeyTags` El control falla si el espacio de claves no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro. `requiredKeyTags` Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y produce un error si el espacio de claves no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a un espacio de claves de Amazon Keyspaces, consulte [Añadir etiquetas a un espacio de claves en la Guía para](#) desarrolladores de Amazon Keyspaces.

Controles de Security Hub para Kinesis

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon Kinesis.

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Kinesis.1] Las transmisiones de Kinesis deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::Kinesis::Stream

Regla de AWS Config : [kinesis-stream-encrypted](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si Kinesis Data Streams está cifrada en reposo con el cifrado del servidor. Este control falla si una transmisión de Kinesis no se cifra en reposo con el cifrado del servidor.

El cifrado del servidor es una característica de Amazon Kinesis Data Streams que cifra automáticamente los datos antes de que estén en reposo mediante un AWS KMS key. Los datos se cifran antes de escribirlos en la capa de almacenamiento del flujo de Kinesis y se descifran después de recuperarlos del almacenamiento. Como resultado, sus datos se cifran en reposo dentro del servicio de Amazon Kinesis Data Streams.

Corrección

Para obtener información sobre cómo habilitar el cifrado del servidor para las transmisiones de Kinesis, consulte [¿Cómo puedo empezar con el cifrado del servidor?](#) en la Guía para desarrolladores de Amazon Kinesis.

[Kinesis.2] Las transmisiones de Kinesis deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Kinesis::Stream

Regla de AWS Config: tagged-kinesis-stream (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un flujo de datos de Amazon Kinesis tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el flujo

de datos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el flujo de datos no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un flujo de datos de Kinesis, consulte [Etiquetado de flujos de Amazon Kinesis Data Streams](#) en la Guía para desarrolladores de Amazon Kinesis.

[Kinesis.3] Las transmisiones de Kinesis deben tener un periodo adecuado de retención de datos

Gravedad: media

Tipo de recurso: `AWS::Kinesis::Stream`

Regla de AWS Config: [kinesis-stream-backup-retention-check](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
minimumBackupRetentionPeriod	Cantidad mínima de horas que deben conservarse los datos.	Cadena	24 a 8760	168

Este control comprueba si un flujo de datos de Amazon Kinesis tiene un periodo de retención de datos más largo o igual de largo que el periodo especificado. El control lanza un error si el periodo de retención de datos es más corto que el periodo especificado. A menos que se proporcione un valor personalizado para el parámetro del periodo de retención de datos, Security Hub utiliza un valor predeterminado de 168 horas.

En Kinesis Data Streams, un flujo de datos es una secuencia ordenada de registros de datos que se puede escribir y leer en tiempo real. Los registros de datos se almacenan temporalmente en particiones de su flujo. El periodo de tiempo desde que se agrega un registro hasta que ya no se puede obtener acceso a él se denomina periodo de retención. Kinesis Data Streams hace que los registros más antiguos que el nuevo periodo de retención sean inaccesibles casi inmediatamente después de reducir el periodo de retención. Por ejemplo, cambiar el periodo de retención de 24 horas a 48 horas implica que los registros añadidos a la secuencia 23 horas y 55 minutos antes seguirán estando disponibles después de que hayan transcurrido 24 horas.

Corrección

Para cambiar el periodo de retención de las copias de seguridad de sus flujos de Kinesis Data Streams, consulte [Change the data retention period](#) en la Guía para desarrolladores de Amazon Kinesis Data Streams.

Controles de Security Hub para AWS KMS

Estos AWS Security Hub controles evalúan el AWS Key Management Service (AWS KMS) servicio y los recursos. Es posible que los controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[KMS.1] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS

Requisitos relacionados: NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (3)

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS::IAM::Policy

Regla de AWS Config : [iam-customer-policy-blocked-kms-actions](#)

Tipo de horario: provocado por un cambio

Parámetros:

- `blockedActionsPatterns`: `kms:ReEncryptFrom`, `kms:Decrypt` (no personalizable)
- `excludePermissionBoundaryPolicy`: `True` (no personalizable)

Comprueba si la versión predeterminada de las políticas gestionadas por los clientes de IAM permite a los directores utilizar las acciones de AWS KMS descifrado en todos los recursos. El control falla si la política está lo suficientemente abierta como para permitir realizar acciones de `kms:Decrypt` o `kms:ReEncryptFrom` en todas las claves de KMS.

El control solo comprueba las claves de KMS en el elemento Recurso y no tiene en cuenta ningún condicional del elemento Condición de una política. Además, el control evalúa las políticas administradas por el cliente asociadas y no asociadas. No comprueba las políticas integradas ni las políticas gestionadas. AWS

Con AWS KMS ella, usted controla quién puede usar sus claves KMS y acceder a sus datos cifrados. Las políticas de IAM definen qué acciones puede realizar una identidad (usuario, grupo o rol) en qué

recursos. Siguiendo las prácticas recomendadas de seguridad, se AWS recomienda conceder los privilegios mínimos. En otras palabras, debe conceder a las identidades únicamente los permisos `kms:Decrypt` o `kms:ReEncryptFrom` y únicamente para las claves que se requieren para realizar una tarea. De lo contrario, es posible que el usuario utilice claves que no sean adecuadas para sus datos.

En lugar de conceder permisos para todas las claves, determine el conjunto mínimo de claves que los usuarios necesitan para acceder a los datos cifrados. Luego, diseñe políticas que permitan a los usuarios usar solo esas claves. Por ejemplo, no permita permisos de `kms:Decrypt` en todas las claves KMS. En su lugar, permita únicamente `kms:Decrypt` las claves de su cuenta en una región determinada. Al adoptar el principio del privilegio mínimo, puede reducir el riesgo de que sus datos se divulguen de forma no intencionada.

Corrección

Para modificar una política de IAM administrada por el cliente, consulte [Edición de políticas gestionadas por el cliente](#) en la Guía del usuario de IAM. Al editar su política, proporcione para el campo `Resource` el nombre de recurso de Amazon (ARN) de la clave o claves específicas en las que desea permitir acciones de descifrado.

[KMS.2] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS

Requisitos relacionados: NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (3)

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso:

- `AWS::IAM::Group`
- `AWS::IAM::Role`
- `AWS::IAM::User`

Regla de AWS Config : [iam-inline-policy-blocked-kms-actions](#)

Tipo de horario: provocado por un cambio

Parámetros:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt` (no personalizable)

Este control comprueba si las políticas integradas en sus identidades de IAM (rol, usuario o grupo) permiten las acciones de AWS KMS descifrado y recifrado de todas las claves de KMS. El control falla si la política está lo suficientemente abierta como para permitir realizar acciones de `kms:Decrypt` o `kms:ReEncryptFrom` en todas las claves de KMS.

El control solo comprueba las claves de KMS en el elemento Recurso y no tiene en cuenta ningún condicional del elemento Condición de una política.

Con él AWS KMS, usted controla quién puede usar sus claves KMS y acceder a sus datos cifrados. Las políticas de IAM definen qué acciones puede realizar una identidad (usuario, grupo o rol) en qué recursos. Siguiendo las prácticas recomendadas de seguridad, se AWS recomienda conceder los privilegios mínimos. En otras palabras, debe conceder a las identidades únicamente los permisos que necesitan y únicamente para las claves que se requieren para realizar una tarea. De lo contrario, es posible que el usuario utilice claves que no sean adecuadas para sus datos.

En lugar de conceder permisos para todas las claves, determine el conjunto mínimo de claves que los usuarios necesitan para acceder a los datos cifrados. Luego, diseñe políticas que permitan a los usuarios usar solo esas claves. Por ejemplo, no permita permisos de `kms:Decrypt` en todas las claves KMS. En su lugar, conceda el permiso solo a claves específicas de una región específica de su cuenta. Al adoptar el principio del privilegio mínimo, puede reducir el riesgo de que sus datos se divulguen de forma no intencionada.

Corrección

Para modificar una política en línea de IAM, consulte [Edición de políticas en línea](#) en la Guía del usuario de IAM. Al editar su política, proporcione para el campo `Resource` el nombre de recurso de Amazon (ARN) de la clave o claves específicas en las que desea permitir acciones de descifrado.

[KMS.3] no AWS KMS keys debe eliminarse involuntariamente

Requisitos relacionados: NIST.800-53.r5 SC-1 2, 2 (NIST.800-53.r5 SC-12)

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Gravedad: crítica

Tipo de recurso: AWS::KMS::Key

Regla de AWS Config : kms-cmk-not-scheduled-for-deletion-2 (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la eliminación de las claves de KMS está programada. El control falla si está programada la eliminación de una clave KMS.

Las claves KMS no se pueden recuperar una vez eliminadas. Los datos cifrados con una clave KMS tampoco se pueden recuperar permanentemente si se elimina la clave KMS. Si los datos significativos se han cifrado con una clave de KMS cuya eliminación está programada, considere la posibilidad de descifrar los datos o volver a cifrarlos con una nueva clave de KMS, a menos que esté realizando un borrado criptográfico de forma intencionada.

Cuando se programa la eliminación de una clave de KMS, se aplica un período de espera obligatorio para dar tiempo a revertir la eliminación, en caso de que se haya programado por error. El período de espera predeterminado es de 30 días, pero se puede reducir a tan solo 7 días si está programada la eliminación de la clave KMS. Durante el período de espera, se puede cancelar la eliminación programada y no se eliminará la clave KMS.

Para obtener información adicional sobre la eliminación de claves de KMS, consulte [Eliminar claves de KMS](#) en la Guía para desarrolladores de AWS Key Management Service .

Corrección

Para cancelar una eliminación de claves de KMS programada, consulte Para cancelar la eliminación de claves en [Programación y cancelación de la eliminación de claves \(consola\)](#) de la Guía para desarrolladores de AWS Key Management Service .

La rotación de AWS KMS teclas [KMS.4] debe estar habilitada

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/3.6, CIS Foundations Benchmark v1.4.0/3.8, CIS AWS Foundations Benchmark v1.2.0/2.8, 2 (NIST.800-53.r5 SC-12), 8 (3), PCI AWS DSS v3.2.1/3.6.4, NIST.800-53.r5 SC-1 PCI DSS v4.0.1/3.7.4 NIST.800-53.r5 SC-2

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS :: KMS :: Key

Regla de AWS Config : [cmk-backing-key-rotation-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

AWS KMS permite a los clientes girar la clave de respaldo, que es el material clave almacenado en AWS KMS y vinculado al ID de clave de la clave KMS. Es la clave de backup que se utiliza para realizar operaciones criptográficas como, por ejemplo, cifrado y descifrado. Actualmente, la rotación de claves automática retiene todas las claves de backup anteriores, por lo que el descifrado de los datos cifrados se puede realizar de forma transparente.

CIS recomienda que habilite la rotación de claves de KMS. La rotación de claves de cifrado ayuda a reducir el impacto potencial de una clave en peligro porque los datos cifrados con una nueva clave no son accesibles con una clave anterior que se haya visto expuesta.

Corrección

Para habilitar la rotación de claves de KMS, consulte [Cómo habilitar y deshabilitar la rotación automática de claves](#) en la Guía para desarrolladores de AWS Key Management Service .

[KMS.5] Las claves KMS no deben ser de acceso público

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: crítica

Tipo de recurso: AWS : : KMS : : Key

Regla de AWS Config : [kms-key-policy-no-public-access](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una AWS KMS key es de acceso público. El control falla si se puede acceder de manera pública a la clave de KMS.

La implementación del acceso con privilegios mínimos es esencial a la hora de reducir los riesgos de seguridad y el impacto de los errores o intentos malintencionados. Si la política de claves de AWS KMS key permite el acceso desde cuentas externas, es posible que terceros puedan cifrar y descifrar los datos con la clave. Esto podría provocar que una amenaza interna o externa extraiga datos del usuario Servicios de AWS que utilice la clave.

 Note

Este control también indica AWS KMS key si las configuraciones AWS Config impiden registrar la política clave en el elemento de configuración (CI) de la clave KMS. FAILED AWS Config Para completar la política clave en el CI para la clave de KMS, el [AWS Config rol](#) debe tener acceso para leer la política clave mediante la llamada a la [GetKeyPolicy](#) API. Para resolver este tipo de problema FAILED, compruebe las políticas que pueden impedir que el AWS Config rol tenga acceso de lectura a la política clave de la clave de KMS. Por ejemplo, compruebe lo siguiente:

- La política clave de la clave KMS.
- [Políticas de control de servicios \(SCPs\)](#) y [políticas de control de recursos \(RCPs\)](#) AWS Organizations que se aplican a su cuenta.
- Permisos para el AWS Config rol, si no usa el rol [AWS Config vinculado al servicio](#).

Además, este control no evalúa las condiciones de la política que utilizan caracteres comodín o variables. Para obtener una PASSED conclusión, las condiciones de la política clave solo deben utilizar valores fijos, que son valores que no contienen caracteres comodín ni variables de política. Para obtener información sobre las variables de política, consulte [Variables y etiquetas](#) en la Guía del AWS Identity and Access Management usuario.

Corrección

Para obtener información sobre cómo actualizar la política clave de una AWS KMS key, consulte [las políticas clave AWS KMS en](#) la Guía para AWS Key Management Service desarrolladores.

Controles de Security Hub para AWS Lambda

Estos AWS Security Hub controles evalúan el AWS Lambda servicio y los recursos. Es posible que los controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Lambda.1] Las políticas de función de Lambda deberían prohibir el acceso público

Requisitos relacionados: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (16) NIST.800-53.r5 AC-6, (20) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4),

NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.4 2.1/7.2.1, PCI DSS v4.0.1/7.2.1 NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: AWS::Lambda::Function

Regla de AWS Config : [lambda-function-public-access-prohibited](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la política basada en recursos de la función de Lambda prohíbe el acceso público a la cuenta. El control falla si se permite el acceso público. El control también falla si se invoca una función de Lambda desde Amazon S3 y la política no incluye una condición para limitar el acceso público, como por ejemplo `AWS:SourceAccount`. Le recomendamos que utilice otras condiciones de S3 junto con `AWS:SourceAccount` en su política de bucket para obtener un acceso más preciso.

Note

Este control no evalúa las condiciones de política que utilizan caracteres comodín o variables. Para obtener un PASSED resultado, las condiciones de la política de la función Lambda solo deben usar valores fijos, que son valores que no contienen caracteres comodín ni variables de política. Para obtener información sobre las variables de política, consulte [Variables y etiquetas](#) en la Guía del AWS Identity and Access Management usuario.

La función de Lambda no debe ser accesible públicamente, ya que puede permitir el acceso involuntario al código que tenga almacenado en la característica.

Corrección

Para solucionar este problema, debe actualizar la política basada en los recursos de su característica para eliminar los permisos o añadir la condición de `AWS:SourceAccount`. Solo puede actualizar la política basada en recursos desde la API Lambda o. AWS CLI

Para empezar, [revise la política basada en recursos de la](#) consola Lambda. Identifique la declaración de política que tiene valores de campo Principal que hacen que la política sea pública, como "*" o { "AWS": "*" }.

No puede editar la política desde la consola. Para eliminar los permisos de la característica, ejecute el comando [remove-permission](#) desde AWS CLI.

```
$ aws lambda remove-permission --function-name <function-name> --statement-id <statement-id>
```

Sustituya *<function-name>* por el nombre de la función de Lambda y *<statement-id>* con el identificador de la sentencia (Sid) que desee eliminar.

[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NiSt.800-53.r5 CM-2, NiSt.800-53.r5 SI-2, NiSt.800-53.r5 SI-2 (2), NiSt.800-53.r5 SI-2 (4), NiSt.800-53.r5 SI-2 (5), PCI DSS v4.0.1/12.3.4

Categoría: Proteger - Desarrollo seguro

Gravedad: media

Tipo de recurso: AWS::Lambda::Function

Regla de AWS Config : [lambda-function-settings-check](#)

Tipo de horario: provocado por un cambio

Parámetros:

- runtime: dotnet8, java21, java17, java11, java8.al2, nodejs22.x, nodejs20.x, nodejs18.x, python3.13, python3.12, python3.11, python3.10, python3.9, ruby3.4, ruby3.3, ruby3.2 (no personalizable)

Este control comprueba si la configuración del tiempo de ejecución de la AWS Lambda función coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. El control falla si la función Lambda no utiliza un tiempo de ejecución compatible, como se indica en la sección Parámetros. Security Hub ignora las funciones que tienen un tipo de paquete de Image.

Los Tiempos de ejecución de Lambda se crean a partir de una combinación de sistema operativo, lenguaje de programación y bibliotecas de software, todos ellos sujetos a operaciones de mantenimiento y actualizaciones de seguridad. Cuando un componente de un tiempo de ejecución deja de recibir actualizaciones de seguridad, Lambda descarta el tiempo de ejecución. Aunque no puede crear funciones que utilicen el tiempo de ejecución obsoleto, la función sigue estando disponible para procesar eventos de invocación. Recomendamos comprobar que sus funciones de Lambda sean actuales y que no utilicen entornos de tiempo de ejecución obsoletos. Para obtener una lista de los tiempos de ejecución compatibles, consulte los [tiempos de ejecución de Lambda](#) en la Guía para desarrolladores de AWS Lambda .

Corrección

Para obtener más información sobre los tiempos de ejecución compatibles y los programas de obsolescencia, consulte la [Política de obsolescencia del tiempo de ejecución](#) en la Guía para desarrolladores de AWS Lambda . Cuando migre los tiempos de ejecución a la versión más reciente, siga la sintaxis y las instrucciones de los editores del lenguaje. También recomendamos implementar [actualizaciones del tiempo de ejecución](#) para ayudar a reducir el riesgo de que las cargas de trabajo se vean afectadas en el caso de que se produzca una incompatibilidad entre las versiones en el tiempo de ejecución.

[Lambda.3] Las funciones de Lambda deben estar en una VPC

Requisitos relacionados: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: baja

Tipo de recurso: AWS::Lambda::Function

AWS Config regla: [lambda-inside-vpc](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si se implementó una función de Lambda en una nube privada virtual (VPC). El control falla si no se implementa la función de Lambda en una VPC. Security Hub no evalúa la configuración de direccionamiento de subred de VPC para determinar la accesibilidad pública. Es posible que vea resultados erróneos en los recursos de Lambda @Edge.

La implementación de recursos en una VPC refuerza la seguridad y el control de las configuraciones de red. Estas implementaciones también ofrecen escalabilidad y una alta tolerancia a los errores en varias zonas de disponibilidad. Puede personalizar las implementaciones de VPC para cumplir con los diversos requisitos de las aplicaciones.

Corrección

Para configurar una característica existente para conectarse a subredes privadas de su VPC, [consulte](#) Configuración del acceso a la VPC en la Guía para desarrolladores de AWS Lambda . Recomendamos elegir al menos dos subredes privadas para una alta disponibilidad y al menos un grupo de seguridad que cumpla con los requisitos de conectividad de la característica.

[Lambda.5] Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.R5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::Lambda::Function

Regla de AWS Config : [lambda-vpc-multi-az-check](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
availabilityZones	Cantidad mínima de zonas de disponibilidad	Enum	2, 3, 4, 5, 6	2

Este control comprueba si una AWS Lambda función que se conecta a una nube privada virtual (VPC) funciona al menos en el número especificado de zonas de disponibilidad (AZs). El control falla si la función no funciona al menos en el número especificado de AZs. A menos que proporciones un valor de parámetro personalizado para el número mínimo de AZs, Security Hub usa un valor predeterminado de dos AZs.

La implementación de recursos en varios AZs es una práctica AWS recomendada para garantizar una alta disponibilidad en su arquitectura. La disponibilidad es un pilar fundamental del modelo de seguridad de la tríada de confidencialidad, integridad y disponibilidad. Todas las funciones de Lambda que se conectan a una VPC deben tener una implementación multi-AZ para garantizar que una sola zona de error no provoque una interrupción total de las operaciones.

Corrección

Si configura la función para conectarse a una VPC de su cuenta, especifique las subredes en varias AZs para garantizar una alta disponibilidad. Para obtener instrucciones, consulte [Configuración del acceso a la VPC](#) en la Guía para desarrolladores de AWS Lambda .

Lambda ejecuta automáticamente otras funciones de forma múltiple AZs para garantizar que esté disponible para procesar eventos en caso de una interrupción del servicio en una sola zona.

[Lambda.6] Las funciones de Lambda deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Lambda::Function

Regla de AWS Config : tagged-lambda-function (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si una AWS Lambda función tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si la función no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si la función no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre

ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una función de Lambda, consulte [Uso de etiquetas en funciones de Lambda](#) en la Guía para desarrolladores de AWS Lambda .

Controles de Security Hub para Macie

Estos AWS Security Hub controles evalúan el servicio Amazon Macie.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Macie.1] Amazon Macie debe estar habilitado

Requisitos relacionados: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CA-7, NIST.800-53.r5 SA-8 (19) NIST.800-53.r5 RA-5, NIST.800-53.R5 SI-4

Categoría: Detectar - Servicios de detección

Gravedad: media

Tipo de recurso: AWS :: Account

Regla de AWS Config : [macie-status-check](#)

Tipo de programa: Periódico

Este control comprueba si Amazon Macie está habilitado para una cuenta. Se produce un error en el control si Macie no está habilitado para la cuenta.

Amazon Macie detecta datos confidenciales mediante el machine learning y la coincidencia de patrones, proporciona visibilidad de los riesgos de seguridad de los datos y permite establecer una protección automatizada contra esos riesgos. Macie evalúa de manera automática y continua los buckets de Amazon Simple Storage Service (Amazon S3) para garantizar la seguridad y el control de acceso, y genera resultados para notificarle posibles problemas con la seguridad o la privacidad de los datos de Amazon S3. Macie también detecta y notifica de manera automática los datos confidenciales, como información de identificación personal (PII), para proporcionarle una mejor

comprensión de los datos que almacena en Amazon S3. Para más información, consulte la [Guía del usuario de Amazon Macie](#).

Corrección

Para habilitar Macie, consulte [Habilitación de Macie](#) en la Guía del usuario de Amazon Macie.

[Macie.2] La detección automática de datos confidenciales de Macie debe estar habilitada

Requisitos relacionados: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9 (1), (19), NIST.800-53.r5 SI-4 NIST.800-53.r5 RA-5 NIST.800-53.r5 SA-8

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: AWS :: Account

Regla de AWS Config : [macie-auto-sensitive-data-discovery-check](#)

Tipo de programa: Periódico

Este control comprueba si la detección automática de datos confidenciales está habilitada en una cuenta de administrador de Amazon Macie. Se produce un error en el control si la detección automática de datos confidenciales no está habilitada en una cuenta de administrador de Macie. Este control solo se aplica a las cuentas de administrador.

Macie detecta y notifica de manera automática los datos confidenciales, como información de identificación personal (PII), en buckets de Amazon Simple Storage Service (Amazon S3). Gracias a la detección automática de datos confidenciales, Macie evalúa continuamente su inventario de buckets y utiliza técnicas de muestreo para identificar y seleccionar los objetos de S3 representativos de sus buckets. A continuación, Macie analiza los objetos seleccionados en busca de datos confidenciales. A medida que el análisis avanza, Macie actualiza las estadísticas, los datos de inventario y demás información que proporciona sobre sus datos en S3. Macie también genera resultados para informar sobre los datos confidenciales que encuentra.

Corrección

Para crear y configurar trabajos automáticos de descubrimiento de datos confidenciales para analizar objetos en buckets de S3, consulte [Configuring automated sensitive data discovery for your account](#) en la Guía del usuario de Amazon Macie.

Controles de Security Hub para Amazon MSK

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon Managed Streaming for Apache Kafka (Amazon MSK).

Es posible que estos controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[MSK.1] Los clústeres de MSK deben cifrarse en tránsito entre los nodos intermediarios

Requisitos relacionados: NIST.800-53.r5 SC-1 3 NIST.800-53.r5 AC-4, 3 (NIST.800-53.r5 SC-23), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 (2), PCI DSS v4.0.1/4.2.1

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::MSK::Cluster

Regla de AWS Config : [msk-in-cluster-node-require-tls](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de Amazon MSK está cifrado en tránsito con HTTPS (TLS) entre los nodos intermediarios del clúster. El control falla si la comunicación de texto sin formato está habilitada para una conexión de nodo intermediario del clúster.

HTTPS ofrece un nivel de seguridad adicional, ya que utiliza el TLS para mover los datos y se puede utilizar para evitar que posibles atacantes utilicen ataques similares para espiar person-in-the-middle o manipular el tráfico de la red. De forma predeterminada, Amazon MSK cifra los datos en tránsito con TLS. Sin embargo, puede anular este valor predeterminado en el momento en que cree el clúster. Recomendamos utilizar conexiones cifradas a través de HTTPS (TLS) para las conexiones de nodos intermediarios.

Corrección

Para actualizar la configuración de cifrado de los clústeres de MSK, consulte [Actualización de la configuración de seguridad de un clúster](#) en la Guía para desarrolladores de Amazon Managed Streaming para Apache Kafka.

[MSK.2] Los clústeres de MSK deberían tener configurada una supervisión mejorada

Requisitos relacionados: NIST.800-53.r5 SI-2 NIST.800-53.r5 CA-7

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::MSK::Cluster

Regla de AWS Config : [msk-enhanced-monitoring-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de Amazon MSK tiene configurada la supervisión mejorada, especificada mediante un nivel de supervisión de al menos PER_TOPIC_PER_BROKER. Se produce un error en el control si el nivel de supervisión del clúster está establecido en DEFAULT o PER_BROKER.

El nivel de supervisión PER_TOPIC_PER_BROKER proporciona información más detallada sobre el rendimiento del clúster de MSK y también proporciona métricas relacionadas con el uso de los recursos, como el uso de la CPU y la memoria. Esto ayuda a identificar los cuellos de botella en el rendimiento y los patrones de uso de los recursos para temas y agentes individuales. Esta visibilidad, a su vez, puede optimizar el rendimiento de sus agentes de Kafka.

Corrección

Para configurar la supervisión mejorada para un clúster de MSK, haga lo siguiente:

1. ¿Abrir la consola Amazon MSK en <https://console.aws.amazon.com/msk/casa?region=us-east-1#/home/>.
2. En el panel de navegación, seleccione Clusters (Clústeres). A continuación, elija una etiqueta de clúster.
3. En Acción, seleccione Editar supervisión.

4. Seleccione la opción Supervisión mejorada a nivel de tema.
5. Elija Guardar cambios.

Para obtener más información sobre los niveles de supervisión, consulte [Actualización de la configuración de seguridad de un clúster](#) en la Guía para desarrolladores de Amazon Managed Streaming para Apache Kafka.

[MSK.3] Los conectores de MSK Connect deben cifrarse en tránsito

Requisitos relacionados: PCI DSS v4.0.1/4.2.1

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::KafkaConnect::Connector

Regla de AWS Config : msk-connect-connector-encrypted (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un conector Amazon MSK Connect está cifrado en tránsito. Este control falla si el conector no está cifrado en tránsito.

Los datos en tránsito hacen referencia a los datos que se mueven de una ubicación a otra, por ejemplo, entre los nodos del clúster o entre el clúster y la aplicación. Los datos pueden moverse a través de Internet o dentro de una red privada. El cifrado de los datos en tránsito reduce el riesgo de que un usuario no autorizado pueda espiar el tráfico de la red.

Corrección

Puede habilitar el cifrado en tránsito cuando crea un conector MSK Connect. No puede cambiar la configuración de cifrado después de crear un conector. Para obtener más información, consulte [Crear un conector](#) en la Guía para desarrolladores de Amazon Managed Streaming para Apache Kafka.

Controles de Security Hub para Amazon MQ

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon MQ.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[MQ.2] Los corredores de ActiveMQ deberían transmitir los registros de auditoría a CloudWatch

Requisitos relacionados: NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-12, NIST.800-53.r5 SI-4, PCI DSS v4.0.1/10.3.3

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::AmazonMQ::Broker

Regla de AWS Config : [mq-cloudwatch-audit-log-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un bróker ActiveMQ de Amazon MQ transmite los registros de auditoría a Amazon Logs. CloudWatch El control falla si el agente no transmite los registros de auditoría a Logs. CloudWatch

Al publicar los registros de ActiveMQ Broker en Logs CloudWatch , puede CloudWatch crear alarmas y métricas que aumenten la visibilidad de la información relacionada con la seguridad.

Corrección

Para transmitir los registros de los corredores de ActiveMQ CloudWatch a los registros, consulte Configuración de [Amazon MQ para los registros de ActiveMQ en la Guía para desarrolladores de Amazon MQ](#).

[MQ.3] Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias

Requisitos relacionados: NIST.800-53.r5 CM-3, NIST.800-53.r5 SI-2, PCI DSS v4.0.1/6.3.3

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: baja

Tipo de recurso: AWS::AmazonMQ::Broker

Regla de AWS Config : [mq-auto-minor-version-upgrade-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un agente de Amazon MQ tiene habilitada la actualización automática de las versiones secundarias. El control falla si el agente no tiene habilitada la actualización automática de las versiones secundarias.

A medida que Amazon MQ publique y admita las nuevas versiones del motor del agente, los cambios son compatibles con versiones anteriores de una aplicación existente y no dan de baja las funciones existentes. Las actualizaciones automáticas de las versiones del motor del agente lo protegen contra los riesgos de seguridad, ayudan a corregir errores y mejoran la funcionalidad.

 Note

Si el agente asociado a la actualización automática de una versión secundaria utiliza el parche más reciente y deja de ser compatible, debe tomar medidas manuales para hacer la actualización.

Corrección

Para habilitar la actualización automática de la versión secundaria para un agente de MQ, consulte [Automatically upgrading the minor engine version](#) en la Guía para desarrolladores de Amazon MQ.

[MQ.4] Los agentes de Amazon MQ deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::AmazonMQ::Broker

Regla de AWS Config : tagged-amazonmq-broker (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un agente de Amazon MQ tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el agente no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el agente no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre

ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un agente de Amazon MQ, consulte [Etiquetado de recursos](#) en la Guía para desarrolladores de Amazon MQ.

[MQ.5] Los corredores ActiveMQ deben usar el modo de implementación activo/en espera

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), Nist.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: baja

Tipo de recurso: AWS::AmazonMQ::Broker

Regla de AWS Config : [mq-active-deployment-mode](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el modo de implementación de un broker ActiveMQ de Amazon MQ está configurado como activo/en espera. El control falla si se establece un corredor de instancia única (habilitado de forma predeterminada) como modo de implementación.

La implementación activa/en espera proporciona una alta disponibilidad para sus corredores ActiveMQ de Amazon MQ en una Región de AWS. El modo de implementación activo/en espera incluye dos instancias de agente en dos zonas de disponibilidad diferentes, configuradas en un par redundante. Estos agentes se comunican de forma sincrónica con la aplicación, lo que puede reducir el tiempo de inactividad y la pérdida de datos en caso de que se produzca un error.

Corrección

Para crear un nuevo agente ActiveMQ con el modo de implementación activo/en espera, consulte [Creación y configuración de un agente ActiveMQ](#) en la Guía para desarrolladores de Amazon

MQ. En Modo de implementación, elija Agente activo/en espera. No se puede cambiar el modo de implementación de un broker ya existente. En su lugar, debe crear un nuevo corredor y copiar la configuración del corredor anterior.

[MQ.6] Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, (2), NIST.800-53.r5 SI-13 NIST.800-53.r5 SC-5 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: baja

Tipo de recurso: AWS::AmazonMQ::Broker

Regla de AWS Config : [mq-rabbit-deployment-mode](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el modo de implementación de un bróker RabbitMQ de Amazon MQ está configurado para la implementación en clúster. El control falla si se establece un corredor de instancia única (habilitado de forma predeterminada) como modo de implementación.

La implementación de clústeres proporciona una alta disponibilidad para sus corredores de Amazon MQ RabbitMQ en una Región de AWS. La implementación del clúster es una agrupación lógica de tres nodos de agente de RabbitMQ, cada uno con su propio volumen de Amazon Elastic Block Store (Amazon EBS) y un estado compartido. La implementación del clúster garantiza que los datos se repliquen en todos los nodos del clúster, lo que puede reducir el tiempo de inactividad y la pérdida de datos en caso de error.

Corrección

Para crear un nuevo bróker de RabbitMQ con el modo de implementación de clústeres, consulte [Creación y conexión a un bróker de RabbitMQ](#) en la Guía para desarrolladores de Amazon MQ. Para el Modo de implementación, elija Implementación en clúster. No se puede cambiar el modo de implementación de un broker ya existente. En su lugar, debe crear un nuevo corredor y copiar la configuración del corredor anterior.

Controles de Security Hub para Neptune

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon Neptune.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [neptune-cluster-encrypted](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de Neptune está cifrado en reposo. El control falla si un clúster de base de datos de Neptune no está cifrado en reposo.

Los datos en reposo se refieren a cualquier dato que se almacene en un almacenamiento persistente y no volátil durante cualquier período de tiempo. El cifrado le ayuda a proteger la confidencialidad de dichos datos, reduciendo el riesgo de que un usuario no autorizado pueda acceder a ellos. El cifrado de sus clústeres de bases de datos de Neptune protege sus datos y metadatos contra el acceso no autorizado. También cumple con los requisitos de conformidad para el data-at-rest cifrado de los sistemas de archivos de producción.

Corrección

Puede habilitar el cifrado en reposo al crear un clúster de base de datos de Neptune. No se puede cambiar la configuración de cifrado después de crear un clúster. Para obtener más información, consulte [Cifrar los recursos inactivos de Neptune](#) en la Guía del usuario de Neptune.

[Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 AU-7(1), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7 Nist.800-53.r5 SI-20, niST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), niST.800-53.r5 SI-4 (20), niST.800-53.r5 SI-4 (5), Nist.800-53.r5 SI-7 (8), PCI DSS v4.0.1/0.1/103,3

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [neptune-cluster-cloudwatch-log-export-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de Neptune publica registros de auditoría en Amazon CloudWatch Logs. El control falla si un clúster de base de datos de Neptune no publica los registros de auditoría en Logs. CloudWatch EnableCloudWatchLogsExport debe estar configurado en. Audit

Amazon Neptune y Amazon CloudWatch están integrados para que pueda recopilar y analizar métricas de rendimiento. Neptune envía automáticamente las métricas a las alarmas CloudWatch y también las admite CloudWatch . Los registros de auditoría son altamente personalizables. Al auditar una base de datos, cada operación realizada con los datos se puede supervisar y registrar en un registro de auditoría que incluye información sobre el clúster de base de datos al que se accede y cómo se accede. Le recomendamos que envíe estos registros para ayudarle CloudWatch a supervisar sus clústeres de base de datos de Neptune.

Corrección

Para publicar registros de auditoría de Neptune en Logs, consulte Publicar CloudWatch registros de [Neptuno CloudWatch en Amazon Logs en](#) la Guía del usuario de Neptune. En la sección Exportaciones de registros, elija Auditar.

[Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas

Requisitos relacionados: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.4.4

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: crítica

Tipo de recurso: AWS::RDS::DBClusterSnapshot

Regla de AWS Config : [neptune-cluster-snapshot-public-prohibited](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instantánea de un clúster de base de datos manual de Neptune es pública. El control falla si una instantánea manual del clúster de base de datos de Neptune es pública.

Una instantánea manual de un clúster de base de datos de Neptune no debe ser pública a menos que se pretenda. Si comparte una instantánea manual sin cifrar públicamente, la instantánea estará disponible para todo Cuentas de AWS. Las instantáneas públicas pueden provocar una exposición no intencionada de los datos.

Corrección

Para eliminar el acceso público a las instantáneas de clústeres de bases de datos manuales de Neptune, consulte [Compartir una instantánea de clúster de base de datos](#) en la Guía del usuario de Neptune.

[Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), (2) NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Gravedad: baja

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [neptune-cluster-deletion-protection-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de Neptune tiene habilitada la protección contra eliminación. El control falla si un clúster de base de datos de Neptune no tiene habilitada la protección contra eliminación.

La activación de la protección contra la eliminación de clústeres ofrece un nivel adicional de protección contra la eliminación accidental de la base de datos o la eliminación por parte de un usuario no autorizado. Un clúster de Neptune DB no se puede eliminar mientras está habilitada la protección contra eliminación. Primero debe deshabilitar la protección contra la eliminación para que la solicitud de eliminación se pueda realizar correctamente.

Corrección

Para habilitar la protección contra la eliminación de un clúster de base de datos de Neptune existente, consulte [Modificación del clúster de base de datos mediante la consola, la CLI y la API](#) en la Guía del usuario de Amazon Aurora.

[Neptune.5] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas

Requisitos relacionados: NIST.800-53.r5 SI-12

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [neptune-cluster-backup-retention-check](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub	
minimumBackupRetentionPeriod	El periodo mínimo de retención de copias de seguridad en días	Entero	De 7 a 35	7	

Este control comprueba si un clúster de base de datos de Neptune tiene las copias de seguridad automáticas habilitadas y un periodo de retención de las copias de seguridad superior o igual al periodo especificado. Se produce un error en el control si las copias de seguridad no están habilitadas para el clúster de base de datos de Neptune o si el periodo de retención es inferior al periodo especificado. A menos que se proporcione un valor personalizado de parámetro para el periodo de retención de copia de seguridad, Security Hub utiliza un valor predeterminado de 7 días.

Las copias de seguridad le ayudan a recuperarse más rápidamente de un incidente de seguridad y a reforzar la resiliencia de sus sistemas. Al automatizar las copias de seguridad de sus clústeres de bases de datos de Neptune, podrá restaurar sus sistemas a un punto en el tiempo y minimizar el tiempo de inactividad y la pérdida de datos.

Corrección

Para habilitar las copias de seguridad automatizadas y establecer un periodo de retención de copias de seguridad para los clústeres de bases de datos de Neptune, consulte [Habilitación de las copias de seguridad automatizadas](#) en la Guía del usuario de Amazon RDS. Para el periodo de retención de la copia de seguridad, elija un valor mayor o igual a 7.

[Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-7 (18)

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::RDS::DBClusterSnapshot

Regla de AWS Config : [neptune-cluster-snapshot-encrypted](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instantánea de un clúster de base de datos de Neptune está cifrada en reposo. El control falla si un clúster de base de datos de Neptune no está cifrado en reposo.

Los datos en reposo se refieren a cualquier dato que se almacene en un almacenamiento persistente y no volátil durante cualquier período de tiempo. El cifrado le ayuda a proteger la confidencialidad de dichos datos, reduciendo el riesgo de que un usuario no autorizado acceda a ellos. Los datos de las instantáneas de los clústeres de base de datos de Neptune deben cifrarse en reposo para ofrecer un nivel de seguridad adicional.

Corrección

No puede cifrar una instantánea de un clúster de base de datos de Neptune existente. En su lugar, debe restaurar la instantánea en un nuevo clúster de base de datos y habilitar el cifrado en el clúster. Puede crear una instantánea cifrada desde el clúster cifrado. Para obtener instrucciones, consulte [Restauración desde una instantánea de clúster de base de datos](#) y [Creación de una instantánea de clúster de base de datos en Neptune](#) en la Guía del usuario de Neptune.

[Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Categoría: Proteger > Gestión del acceso seguro > Autenticación sin contraseña

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [neptune-cluster-iam-database-authentication](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de Neptune tiene habilitada la autenticación de bases de datos de IAM. El control falla si la autenticación de la base de datos de IAM no está habilitada para un clúster de base de datos de Neptune.

La autenticación de base de datos de IAM para los clústeres de base de datos de Amazon Neptune elimina la necesidad de almacenar credenciales de usuario en la configuración de base de datos, ya que la autenticación se administra externamente mediante IAM. Cuando la autenticación de bases de datos de IAM está habilitada, cada solicitud debe firmarse con la versión 4 de AWS Signature.

Corrección

De forma predeterminada, la autenticación de bases de datos de IAM está deshabilitada al crear un clúster de Neptune DB. Para habilitarlo, consulte [Habilitar la autenticación de bases de datos de IAM en Neptune](#) en la Guía del usuario de Neptune.

[Neptune.8] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [neptune-cluster-copy-tags-to-snapshot-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de Neptune está configurado para copiar todas las etiquetas en las instantáneas cuando se crean las instantáneas. El control falla si un clúster de base de datos de Neptune no está configurado para copiar etiquetas a las instantáneas.

La identificación y el inventario de sus activos de TI es un aspecto fundamental de seguridad y control. Debe etiquetar instantáneas del mismo modo que los clústeres de base de datos de Amazon

RDS principales. La copia de las etiquetas garantiza que los metadatos para las instantáneas de base de datos coincidan con los clústeres de base de datos principales y que cualquier política de acceso para la instantánea de base de datos también coincida con la de la instancia de base de datos principal.

Corrección

Para copiar etiquetas en instantáneas de clústeres de bases de datos de Neptune, [consulte Copiar etiquetas en Neptune](#) en la Guía del usuario de Neptune.

[Neptune.9] Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad

Requisitos relacionados: 6, NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 (2 NIST.800-53.r5 SC-5), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [neptune-cluster-multi-az-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de Amazon Neptune tiene instancias de lectura y réplica en varias zonas de disponibilidad (). AZs Se produce un error en el control si el clúster se implementa en una sola AZ.

Si una AZ no está disponible y durante los eventos de mantenimiento habituales, las réplicas de lectura sirven como destinos de conmutación por error para la instancia principal. Es decir, si la instancia principal falla, Neptune promueve una instancia de réplica de lectura para convertirla en la instancia primaria. Por el contrario, si su clúster de base de datos no incluye ninguna instancia de réplica de lectura, su clúster de base de datos seguirá sin estar disponible cuando la instancia principal falle hasta que se vuelva a crear. Volver a crear la instancia principal lleva mucho más tiempo que promover una réplica de lectura. Para garantizar una alta disponibilidad, le recomendamos que cree una o más instancias de réplica de lectura que tengan la misma clase de

instancia de base de datos que la instancia principal y que estén ubicadas en una instancia diferente AZs a la principal.

Corrección

Para implementar un clúster de base de datos Neptune en varios AZs, consulte [Lectura y réplica de instancias de base de datos en un clúster de base de datos Neptune en la Guía del usuario de Neptune](#).

Controles de Security Hub para AWS Network Firewall

Estos AWS Security Hub controles evalúan el AWS Network Firewall servicio y los recursos. Es posible que los controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

Los NetworkFirewall firewalls de Network Firewall se deben implementar en varias zonas de disponibilidad

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::NetworkFirewall::Firewall

Regla de AWS Config : [netfw-multi-az-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control evalúa si un firewall administrado mediante AWS Network Firewall se implementa en varias zonas de disponibilidad (AZs). Se produce un error en el control si un firewall se implementa en una sola AZ.

AWS La infraestructura global de incluye varias Regiones de AWS. AZs son ubicaciones físicamente independientes y aisladas de cada región que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Al implementar un firewall de Network Firewall en varias AZs zonas, puede equilibrar y desviar el tráfico entre ellas AZs, lo que ayuda a diseñar soluciones de alta disponibilidad.

Corrección

Implementación de un firewall de Network Firewall en varias zonas de AZs

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, en Firewall de red, elija Firewalls.
3. En la página Firewalls, seleccione el nombre del firewall que quiere editar.
4. En la página de detalles del firewall, elija la pestaña Detalles del firewall.
5. En la sección Política asociada y VPC, elija Editar
6. Para agregar una nueva AZ, elija Agregar nueva subred. Seleccione la AZ y la subred que quiere utilizar. Seleccione al menos dos AZs.
7. Seleccione Save.

[NetworkFirewall.2] El registro de Network Firewall debe estar habilitado

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), (4), (26), (9), NIST.800-53.r5 SI-3 NIST.800-53.r5 AC-2 (8), NIST.800-53.r5 SI-4, NIST.800-53.r5 AC-4 NIST.800-53.r5 SI-4 NIST.800-53.r5 AC-6 (20), NIST.800-53.r5 SI-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-171.r5 SI-7 NIST.800-53.r5 SC-7 (8), NIST.800-173.r5 SI-7 (8), NIST.800-173.r5 SI-7 (8), NIST.800-173.r5 SI-7 (8), NIST.800-173.r5 SI-7 (8), NIST.800-173.r5 SI-7 (8), NIST.800-173.r5 SI-7 (8), NIST.800-173.r5 SI-7 (8), NIST.800-173.r3,1131

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::NetworkFirewall::LoggingConfiguration

Regla de AWS Config : [netfw-logging-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el registro está habilitado para un AWS Network Firewall firewall de. Se produce un error en el control si el registro no está habilitado para al menos un tipo de registro o si el destino del registro no existe.

El registro ayuda a mantener la fiabilidad, la disponibilidad y el rendimiento de los firewalls. En Network Firewall, el registro proporciona información detallada sobre el tráfico de red, incluida la hora en la que el motor con estado recibió un flujo de paquetes, información detallada acerca del flujo de paquetes y las medidas de regla de estado adoptadas respecto del flujo de paquetes.

Corrección

Para habilitar el registro en un firewall, consulte [Updating a firewall's logging configuration](#) en la Guía para desarrolladores de AWS Network Firewall .

[NetworkFirewall.3] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-171.r2 3.r5 CM-2, NIST.800-171.r2 3.r5 CM-2, NIST.800-171.r2 3.r5 CM-2, NIST.800-171.r2 3.r2 3.1

Categoría: Proteger > Configuración de red segura

Gravedad: media

Tipo de recurso: AWS::NetworkFirewall::FirewallPolicy

Regla de AWS Config : [netfw-policy-rule-group-associated](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una política de Network Firewall tiene asociados grupos de reglas con estado o sin estado. El control falla si no se asignan grupos de reglas sin estado o con estado.

Una política de firewall define la forma en que su firewall supervisa y gestiona el tráfico en Amazon Virtual Private Cloud (Amazon VPC). La configuración de grupos de reglas con estado y sin estado ayuda a filtrar los paquetes y los flujos de tráfico, y define el manejo del tráfico predeterminado.

Corrección

Para añadir un grupo de reglas a una política de Network Firewall, consulte [Actualización de una política de firewall](#) en la Guía para desarrolladores de AWS Network Firewall . Para obtener información sobre cómo crear y administrar grupos de reglas, consulte [Grupos de reglas en AWS Network Firewall](#).

[NetworkFirewall.4] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Proteger > Configuración de red segura

Gravedad: media

Tipo de recurso: AWS::NetworkFirewall::FirewallPolicy

Regla de AWS Config : [netfw-policy-default-action-full-packets](#)

Tipo de horario: provocado por un cambio

Parámetros:

- `statelessDefaultActions`: `aws:drop,aws:forward_to_sfe` (no personalizable)

Este control comprueba si la acción sin estado predeterminada para los paquetes completos de una política de Network Firewall es eliminar o reenviar. El control se activa si se selecciona Drop o Forward, y da error si se selecciona Pass.

Una política de firewall define la forma en que su firewall supervisa y gestiona el tráfico en Amazon VPC. Puede configurar grupos de reglas sin estado y con estado para filtrar los paquetes y los flujos de tráfico. Si se establece de forma predeterminada a Pass se puede permitir el tráfico no deseado.

Corrección

Para cambiar la política de firewall, consulte [Actualización de una política de firewall](#) en la Guía para desarrolladores de AWS Network Firewall . Para las Acciones predeterminadas Sin estado, seleccione Editar. A continuación, seleccione Soltar o Reenviar a grupos de reglas con estado como Acción.

[NetworkFirewall.5] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-171.r2 3.r5 CM-2, NIST.800-53.r5 CM-2, NIST.800-171.r2 3.1, NIST.800-171.r2 3.r5 CM-2

Categoría: Proteger > Configuración de red segura

Gravedad: media

Tipo de recurso: AWS::NetworkFirewall::FirewallPolicy

Regla de AWS Config : [netfw-policy-default-action-fragment-packets](#)

Tipo de horario: provocado por un cambio

Parámetros:

- statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe (no personalizable)

Este control comprueba si la acción sin estado predeterminada para los paquetes fragmentados de una política de Network Firewall es eliminar o reenviar. El control se activa si se selecciona Drop o Forward, y da error si se selecciona Pass.

Una política de firewall define la forma en que su firewall supervisa y gestiona el tráfico en Amazon VPC. Puede configurar grupos de reglas sin estado y con estado para filtrar los paquetes y los flujos de tráfico. Si se establece de forma predeterminada a Pass se puede permitir el tráfico no deseado.

Corrección

Para cambiar la política de firewall, consulte [Actualización de una política de firewall](#) en la Guía para desarrolladores de AWS Network Firewall . Para las Acciones predeterminadas Sin estado, seleccione Editar. A continuación, seleccione Soltar o Reenviar a grupos de reglas con estado como Acción.

El grupo de reglas de Stateless Network Firewall [NetworkFirewall.6] no debe estar vacío

Requisitos relacionados: NIST.800-53.r5 AC-4 (21), (11), (16) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-53.r5 SC-7 NIST.800-171.r2 3.r2 3.14, NIST.800-171.r2 3.1, NIST.800-171.r2 3.1, NIST.800-171.r2 3.r2 3.6 NIST.800-53.r5 SC-7

Categoría: Proteger > Configuración de red segura

Gravedad: media

Tipo de recurso: AWS::NetworkFirewall::RuleGroup

Regla de AWS Config : [netfw-stateless-rule-group-not-empty](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de reglas sin estado en AWS Network Firewall contiene reglas. El control falla si no hay reglas en el grupo de reglas.

Un grupo de reglas contiene reglas que definen cómo el firewall procesa el tráfico en la VPC. Un grupo de reglas sin estado vacío, cuando está presente en una política de cortafuegos, puede dar la impresión de que el grupo de reglas procesará tráfico. Sin embargo, cuando el grupo de reglas sin estado está vacío, no procesa el tráfico.

Corrección

Para agregar reglas a su grupo de reglas de Network Firewall, consulte [Actualización de un grupo de reglas con estado](#) en la Guía para desarrolladores de AWS Network Firewall . En la página de detalles del firewall, en el Grupo de reglas sin estado, seleccione Editar para añadir reglas.

Los NetworkFirewall firewalls de Network Firewall se deben etiquetar

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::NetworkFirewall::Firewall

Regla de AWS Config : tagged-networkfirewall-firewall (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas	No default value

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.		que cumplan con AWS los requisitos .	

Este control comprueba si un AWS Network Firewall firewall de tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el firewall no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el firewall no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un firewall de Network Firewall, consulte [Etiquetado de AWS Network Firewall recursos](#) de en la Guía para AWS Network Firewall desarrolladores de.

[NetworkFirewall.8] Las políticas de firewall de Network Firewall se deben etiquetar

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::NetworkFirewall::FirewallPolicy

Regla de AWS Config : tagged-networkfirewall-firewallpolicy (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si una política de AWS Network Firewall firewall de tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si la política de firewall no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la política de firewall no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Las etiquetas se pueden asignar a los AWS recursos de y constan de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a AWS recursos de. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Qué es ABAC para? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles para muchos Servicios de AWS, incluido AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una política de Network Firewall, consulte [Etiquetado de AWS Network Firewall recursos](#) en la Guía para AWS Network Firewall desarrolladores.

Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de eliminación

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoría: Proteger > Seguridad de red

Gravedad: media

Tipo de recurso: AWS::NetworkFirewall::Firewall

Regla de AWS Config : [netfw-deletion-protection-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un AWS Network Firewall firewall de tiene habilitada la protección de eliminación. El control falla si la protección contra la eliminación no está habilitada en un firewall.

AWS Network Firewall es un servicio de detección de intrusiones y firewall de red gestionado y con estado que le permite inspeccionar y filtrar el tráfico hacia sus nubes privadas virtuales (VPCs), desde ellas o entre ellas. La configuración de protección contra la eliminación protege contra la eliminación accidental del firewall.

Corrección

Para habilitar la protección contra eliminación en un firewall de Network Firewall existente, consulte [Actualización de un firewall](#) en la Guía para desarrolladores de AWS Network Firewall . Para Cambiar las protecciones, seleccione Habilitar. También puede activar la protección contra la eliminación invocando la [UpdateFirewallDeleteProtection](#) API y configurando el campo `enDeleteProtection`.
`true`

Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de cambio de subred

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoría: Proteger > Seguridad de red

Gravedad: media

Tipo de recurso: `AWS::NetworkFirewall::Firewall`

Regla de AWS Config : [netfw-subnet-change-protection-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la protección contra cambios de subred está habilitada para un AWS Network Firewall firewall de. El control lanza un error si la protección contra cambios de subred no está habilitada para el firewall de.

AWS Network Firewall es un servicio de detección de intrusiones y firewall de red gestionado y con estado que puede utilizar para inspeccionar y filtrar el tráfico hacia sus nubes privadas virtuales

()VPCs, desde ellas o entre ellas. Si habilita la protección contra cambios de subred para un firewall de Network Firewall, puede proteger el firewall contra cambios accidentales en las asociaciones de subred del firewall.

Corrección

Para obtener información sobre cómo habilitar la protección contra cambios de subred para un firewall de Network Firewall existente, consulte [Actualización de un firewall](#) en la Guía para AWS Network Firewall desarrolladores.

Controles de Security Hub para Amazon OpenSearch Service

Estos AWS Security Hub controles evalúan el OpenSearch servicio y los recursos de Amazon OpenSearch Service (Servicio). Es posible que los controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

Los OpenSearch dominios [Opensearch.1] deben tener activado el cifrado en reposo

Requisitos relacionados: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/7.2.1, (1), 3, 8, 8 (1), NIST.800-53.r5 SI-7 (6) NIST.800-53.r5 CA-9 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-2

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::OpenSearch::Domain

Regla de AWS Config : [opensearch-encrypted-at-rest](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si OpenSearch los dominios tienen habilitada encryption-at-rest la configuración. La comprobación falla si el cifrado en reposo no está habilitado.

Para añadir un nivel de seguridad adicional a los datos confidenciales, debe configurar su dominio de OpenSearch servicio para que esté cifrado en reposo. Al configurar el cifrado de datos en reposo, AWS KMS almacena y administra las claves de cifrado. Para realizar el cifrado, AWS KMS utiliza el algoritmo del estándar de cifrado avanzado con claves de 256 bits (AES-256).

Para obtener más información sobre el cifrado de OpenSearch servicios en reposo, consulte [Cifrado de datos en reposo para Amazon OpenSearch Service](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

Corrección

Para habilitar el cifrado en reposo para OpenSearch dominios nuevos y existentes, consulta [Cómo habilitar el cifrado de datos en reposo](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

Los OpenSearch dominios [Opensearch.2] no deben ser de acceso público

Requisitos relacionados: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7), (21), (11), (16), (20) NIST.800-53.r5 AC-3, (21) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (3), (4) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoría: Proteger > Configuración de red segura > Recursos dentro de VPC

Gravedad: crítica

Tipo de recurso: AWS::OpenSearch::Domain

Regla de AWS Config : [opensearch-in-vpc-only](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si OpenSearch los dominios están en una VPC. No evalúa la configuración de direccionamiento de subred de VPC para determinar el acceso público.

Debe asegurarse de que OpenSearch los dominios no estén conectados a subredes públicas. Consulta [las políticas basadas en recursos](#) en la Guía para desarrolladores de Amazon OpenSearch Service. También debe asegurarse de que la VPC esté configurada de acuerdo con las prácticas recomendadas. Consulte [Prácticas recomendadas de seguridad para su VPC](#) en la Guía del usuario de Amazon VPC.

OpenSearch los dominios implementados en una VPC pueden comunicarse con los recursos de la VPC a través de la AWS red privada, sin necesidad de atravesar la Internet pública. Esta

configuración aumenta la seguridad al limitar el acceso a los datos en tránsito. VPCs proporcionan una serie de controles de red para proteger el acceso a los OpenSearch dominios, incluidas las ACL de red y los grupos de seguridad. Security Hub recomienda migrar OpenSearch los dominios públicos VPCs a para aprovechar estos controles.

Corrección

Si crea un dominio con un punto de enlace público, no podrá colocarlo posteriormente en una VPC. En lugar de ello, se debe crear un dominio nuevo y migrar los datos. y viceversa. Si crea un dominio dentro de una VPC, no puede tener un punto de enlace público. En su lugar, debe [crear otro dominio](#) o deshabilitar este control.

Para obtener instrucciones, consulta Cómo [lanzar tus dominios de Amazon OpenSearch Service dentro de una VPC](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

Los OpenSearch dominios [Opensearch.3] deben cifrar los datos enviados entre nodos

Requisitos relacionados: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 3 (NIST.800-53.r5 SC-23), NIST.800-53.r5 SC-7 (4), (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2) NIST.800-53.r5 SC-8

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::OpenSearch::Domain

Regla de AWS Config : [opensearch-node-to-node-encryption-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si OpenSearch los dominios tienen el node-to-node cifrado activado. Este control falla si el node-to-node cifrado está deshabilitado en el dominio.

El HTTPS (TLS) se puede utilizar para evitar que posibles atacantes escuchen o manipulen el tráfico de la red mediante ataques o similares. person-in-the-middle Solo se deben permitir las conexiones cifradas a través de HTTPS (TLS). Al habilitar el node-to-node cifrado de los OpenSearch dominios, se garantiza que las comunicaciones dentro del clúster se cifren durante el tránsito.

Puede haber una penalización en el rendimiento asociada a esta configuración. Debe conocer y probar la compensación de rendimiento antes de activar esta opción.

Corrección

Para habilitar el node-to-node cifrado en un OpenSearch dominio, consulta [Habilitar el node-to-node cifrado](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

El registro de errores de OpenSearch dominio [Opensearch.4] en CloudWatch Logs debe estar activado

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), Nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.r5 SI-4 (20), Nist.800-53.r5 SI-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::OpenSearch::Domain

Regla de AWS Config : [opensearch-logs-to-cloudwatch](#)

Tipo de horario: provocado por un cambio

Parámetros:

- logtype = 'error' (no personalizable)

Este control comprueba CloudWatch si los dominios están configurados para enviar registros de errores a Logs. OpenSearch Este control falla si el registro de errores no CloudWatch está habilitado para un dominio.

Debe habilitar los registros de errores para OpenSearch los dominios y enviarlos a CloudWatch Logs para su conservación y respuesta. Los registros de errores de los dominios pueden ayudar con las auditorías de seguridad y acceso, y pueden ayudar a diagnosticar problemas de disponibilidad.

Corrección

Para habilitar la publicación de registros, consulta [Habilitar la publicación de registros \(consola\)](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

Los OpenSearch dominios [Opensearch.5] deben tener habilitado el registro de auditoría

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), Nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, Nist.800-53.r5 SI-4 (20), Nist.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::OpenSearch::Domain

Regla de AWS Config : [opensearch-audit-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros:

- `cloudWatchLogsLogGroupArnList` (no personalizable): Security Hub no completa este parámetro. Lista CloudWatch de grupos de registros separados por comas que deben configurarse para los registros de auditoría.

Este control comprueba si los OpenSearch dominios tienen habilitado el registro de auditoría. Este control produce un error si un OpenSearch dominio no tiene activado el registro de auditoría.

Los registros de auditoría son altamente personalizables. Le permiten realizar un seguimiento de la actividad de los usuarios en sus OpenSearch clústeres, incluidos los aciertos y los errores de autenticación, las solicitudesOpenSearch, los cambios de indexación y las consultas de búsqueda entrantes.

Corrección

Para obtener instrucciones sobre cómo habilitar los registros de auditoría, consulta [Habilitar los registros de auditoría](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

Los OpenSearch dominios [Opensearch.6] deben tener al menos tres nodos de datos

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), niST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::OpenSearch::Domain

Regla de AWS Config : [opensearch-data-node-fault-tolerance](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los OpenSearch dominios están configurados con al menos tres nodos de datos y lo está. `zoneAwarenessEnabled true` Este control falla para un OpenSearch dominio si `instanceCount` es menor que 3 o `zoneAwarenessEnabled` es `false`.

Para lograr una alta disponibilidad y tolerancia a errores a nivel de clúster, un OpenSearch dominio debe tener al menos tres nodos de datos. La implementación de un OpenSearch dominio con al menos tres nodos de datos garantiza las operaciones del clúster en caso de que un nodo falle.

Corrección

Para modificar la cantidad de nodos de datos de un OpenSearch dominio

1. Inicia sesión en la AWS consola y abre la consola OpenSearch de Amazon Service en <https://console.aws.amazon.com/aos/>.
2. En Mis dominios, elija el nombre del dominio que desee editar y elija Editar.
3. En Nodos de datos, establezca Número de nodos en un número superior a 3. Si va a realizar la implementación en tres zonas de disponibilidad, establezca el número en un múltiplo de tres para garantizar una distribución equitativa entre las zonas de disponibilidad.
4. Elija Enviar.

Los OpenSearch dominios [Opensearch.7] deben tener habilitado un control de acceso detallado

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6

Categoría: Proteger > Gestión del acceso seguro > Acciones confidenciales de la API restringidas

Gravedad: alta

Tipo de recurso: AWS::OpenSearch::Domain

Regla de AWS Config : [opensearch-access-control-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si OpenSearch los dominios tienen habilitado el control de acceso detallado. El control falla si el control de acceso detallado no está habilitado. El control de acceso detallado requiere advanced-security-options que el parámetro esté habilitado. OpenSearch update-domain-config

El control de acceso detallado ofrece formas adicionales de controlar el acceso a tus datos en Amazon Service. OpenSearch

Corrección

Para habilitar un control de acceso detallado, consulta Control de [acceso detallado en Amazon Service en la Guía para desarrolladores OpenSearch de Amazon Service](#). OpenSearch

[Opensearch.8] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 NIST.800-53.r5 IA-5 (3), 3, 3 (3), NIST.800-53.r5 SC-1 (NIST.800-53.r5 SC-23), NIST.800-53.r5 SC-2 (4), (1), NIST.800-53.r5 SC-7 (2) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6)

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::OpenSearch::Domain

Regla de AWS Config : [opensearch-https-required](#)

Tipo de horario: provocado por un cambio

Parámetros:

- `tlsPolicies`: Policy-Min-TLS-1-2-PFS-2023-10 (no personalizable)

Este control comprueba si un punto de enlace de dominio de Amazon OpenSearch Service está configurado para utilizar la política de seguridad TLS más reciente. El control falla si el punto de enlace del OpenSearch dominio no está configurado para usar la última política compatible o si HTTPS no está habilitado.

El protocolo HTTPS (TLS) se puede utilizar para evitar que posibles atacantes utilicen ataques similares para espiar person-in-the-middle o manipular el tráfico de la red. Solo se deben permitir las conexiones cifradas a través de HTTPS (TLS). El cifrado de los datos en tránsito puede afectar al rendimiento. Debe probar su aplicación con esta característica para comprender el perfil de rendimiento y el impacto del TLS. TLS 1.2 proporciona varias mejoras de seguridad con respecto a las versiones anteriores de TLS.

Corrección

Para habilitar el cifrado TLS, utilice la operación API. [UpdateDomainConfig](#) Configure el [DomainEndpointOptions](#) campo para especificar el valor de `TLSSecurityPolicy`. Para obtener más información, consulta el [Node-to-node cifrado](#) en la Guía para desarrolladores OpenSearch de Amazon Service.

Los OpenSearch dominios [Opensearch.9] deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::OpenSearch::Domain`

Regla de AWS Config : `tagged-opensearch-domain` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas	No default value

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.		que cumplan con AWS los requisitos .	

Este control comprueba si un dominio de Amazon OpenSearch Service tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el dominio no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el dominio no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un dominio OpenSearch de servicio, consulta Cómo [trabajar con etiquetas](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

Los OpenSearch dominios [Opensearch.10] deben tener instalada la última actualización de software

Requisitos relacionados: NIST.800-53.r5 SI-2, niST.800-53.r5 SI-2 (2), niST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: baja

Tipo de recurso: AWS::OpenSearch::Domain

Regla de AWS Config : [opensearch-update-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un dominio de Amazon OpenSearch Service tiene instalada la última actualización de software. Se produce un error en el control si hay una actualización de software disponible, pero no está instalada para el dominio.

OpenSearch Las actualizaciones de software de servicio proporcionan las últimas correcciones, actualizaciones y funciones de plataforma disponibles para el entorno. Mantener la instalación up-to-date de los parches ayuda a mantener la seguridad y la disponibilidad del dominio. Si no se adoptan medidas respecto de las actualizaciones necesarias, actualizaremos el software de servicio automáticamente después de un tiempo determinado (por lo general, dos semanas). Recomendamos programar las actualizaciones en momentos de poco tráfico en el dominio para minimizar las interrupciones del servicio.

Corrección

Para instalar actualizaciones de software para un OpenSearch dominio, consulta Cómo [iniciar una actualización](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

Los OpenSearch dominios [Opensearch.11] deben tener al menos tres nodos principales dedicados

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-3 6, niST.800-53.r5 SI-13

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: baja

Tipo de recurso: AWS::OpenSearch::Domain

Regla de AWS Config : [opensearch-primary-node-fault-tolerance](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un dominio de Amazon OpenSearch Service está configurado con al menos tres nodos principales dedicados. El control falla si el dominio tiene menos de tres nodos principales dedicados.

OpenSearch El servicio utiliza nodos principales dedicados para aumentar la estabilidad del clúster. Un nodo principal dedicado realiza tareas de administración de clústeres, pero no contiene datos ni responde a las solicitudes de carga de datos. Le recomendamos que utilice Multi-AZ con modo de espera, lo que añade tres nodos principales dedicados a cada OpenSearch dominio de producción.

Corrección

Para cambiar el número de nodos principales de un OpenSearch dominio, consulte [Creación y gestión de dominios de Amazon OpenSearch Service](#) en la Guía para desarrolladores de Amazon OpenSearch Service.

Controles de Security Hub para AWS Private CA

Estos AWS Security Hub controles evalúan el AWS Private Certificate Authority (AWS Private CA) servicio y los recursos.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

La autoridad emisora de certificados AWS Private CA raíz [PCA.1] debe estar deshabilitada

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Proteger - Configuración de red segura

Gravedad: baja

Tipo de recurso: AWS::ACMPCA::CertificateAuthority

Regla de AWS Config : [acm-pca-root-ca-disabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si AWS Private CA tiene una autoridad de certificación (CA) raíz deshabilitada. Se produce un error en el control si la autoridad emisora de certificados raíz está habilitada.

Con AWS Private CA, puede crear una jerarquía de CA que incluya una CA raíz y una subordinada. Debe minimizar el uso de la autoridad emisora de certificados raíz para las tareas diarias, especialmente en los entornos de producción. La CA raíz solo debe usarse para emitir certificados para empresas intermedias CAs. Esto permite almacenar la CA raíz de forma segura mientras la entidad emisora intermedia CAs realiza la tarea diaria de emitir los certificados de la entidad final.

Corrección

Para deshabilitar la autoridad emisora de certificados raíz, consulte [Actualización del estado de CA](#) en la Guía del usuario de AWS Private Certificate Authority .

[PCA.2] Se debe etiquetar a las autoridades certificadoras de CA AWS privadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::ACMPCA::CertificateAuthority

Regla de AWS Config : acmpca-certificate-authority-tagged

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una entidad emisora de certificados AWS privada tiene etiquetas con las claves específicas definidas en el parámetro `requiredKeyTags`. El control produce un error si la entidad emisora de certificados no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredKeyTags`. Si `requiredKeyTags` no se proporciona el parámetro, el control solo comprueba la existencia de una clave de etiqueta y produce un error si la autoridad de certificación no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [Definir permisos en función de los atributos con la autorización ABAC](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas. AWS Billing Para obtener más información sobre las mejores prácticas de etiquetado, consulte [las mejores prácticas y estrategias](#) en los AWS recursos de etiquetado y en la Guía del usuario del editor de etiquetas.

Corrección

Para añadir etiquetas a una autoridad de CA AWS privada, consulte [Añadir etiquetas para una entidad de certificación privada](#) en la Guía del AWS Private Certificate Authority usuario.

Controles de Security Hub para Amazon RDS

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon Relational Database Service (Amazon RDS). Es posible que los controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[RDS.1] La instantánea de RDS debe ser privada

Requisitos relacionados: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7), (21), (11), (16), (20) NIST.800-53.r5 AC-3, (21) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (3), (4) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: AWS::RDS::DBClusterSnapshot, AWS::RDS::DBSnapshot

Regla de AWS Config : [rds-snapshots-public-prohibited](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las instantáneas de Amazon RDS son públicas. El control falla si las instantáneas de RDS son públicas. Este control evalúa instancias de RDS, instancias de base de datos de Aurora, instancias de base de datos de Neptune y clústeres de Amazon DocumentDB.

Las instantáneas de RDS se utilizan para realizar copias de seguridad de los datos de las instancias de RDS en un momento determinado. Se pueden utilizar para restaurar estados anteriores de instancias de RDS.

Una instantánea de RDS no debe ser pública a menos que se quiera. Si comparte una instantánea manual sin cifrar públicamente, estará disponible para todas las cuentas de Cuentas de AWS. Esto puede provocar una exposición no intencionada de los datos de su instancia de RDS.

Tenga en cuenta que si se cambia la configuración para permitir el acceso público, es posible que la AWS Config regla no pueda detectar el cambio hasta dentro de 12 horas. Hasta que la AWS Config regla detecte el cambio, la comprobación se realizará aunque la configuración infrinja la regla.

Para obtener más información sobre cómo compartir una instantánea de base de datos, consulte [Cómo compartir una instantánea de base de datos](#) en la Guía del usuario de Amazon RDS.

Corrección

Para eliminar el acceso público de las instantáneas de RDS, consulte [Compartir una instantánea](#) en la Guía del usuario de Amazon RDS. En Visibilidad de las instantáneas de base de datos, elija Privada.

[RDS.2] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.3.3, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-4, (11), (16) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PPCI DSS v3.2.1/7.2.1, PCI DSS v4.0.1/1.4.4

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [rds-instance-public-access-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las instancias de Amazon RDS son accesibles públicamente mediante la evaluación del campo `PubliclyAccessible` en el elemento de configuración de instancia.

Las instancias de base de datos de Neptune y los clústeres de Amazon DocumentDB no tienen el indicador de `PubliclyAccessible` y no se pueden evaluar. Sin embargo, este control aún puede generar resultados para estos recursos. Puede suprimir estos resultados.

El valor `PubliclyAccessible` de la configuración de la instancia de RDS indica si la instancia de base de datos es accesible públicamente. Si la instancia de base de datos se ha configurado con `PubliclyAccessible`, se trata de una instancia orientada a Internet con un nombre DNS que se puede resolver públicamente y que se resuelve en una dirección IP pública. Cuando la instancia de base de datos no es accesible públicamente, se trata de una instancia interna con un nombre DNS que se resuelve en una dirección IP privada.

A menos que tenga la intención de dar acceso público a su instancia de RDS, la instancia de RDS no debe configurarse con el valor `PubliclyAccessible`. Si lo hace, podría generar tráfico innecesario a su instancia de base de datos.

Corrección

Para eliminar el acceso público a las instancias de base de datos de RDS, consulte [Modificación de una instancia de base de datos de Amazon RDS](#) en la Guía del usuario de Amazon RDS. En Acceso público, elija No.

[RDS.3] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.3.1, CIS AWS Foundations Benchmark v1.4.0/2.3.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 NIST.800-53.r5 SC-2 8, 8 NIST.800-53.r5 SC-7 (1), (10), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [rds-storage-encrypted](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el cifrado de almacenamiento está habilitado para las instancias de base de datos de Amazon RDS.

Este control está diseñado para instancias de base de datos de RDS. Sin embargo, también puede generar resultados para instancias de base de datos de Aurora, instancias de base de datos de Neptune y clústeres de Amazon DocumentDB. Si estos resultados no son útiles, puede suprimirlos.

Para obtener una capa adicional de seguridad para la información confidencial en las instancias de base de datos de RDS, debe configurar las instancias de base de datos de RDS de tal manera que se cifren en reposo. Para cifrar las instancias de base de datos de RDS y las instantáneas en reposo, debe habilitar la opción de cifrado para las instancias de base de datos de RDS. Los datos cifrados en reposo incluyen el almacenamiento subyacente de una instancia de base de datos, sus copias de seguridad automatizadas, sus réplicas de lectura y sus instantáneas.

En las instancias de base de datos cifradas de RDS se utiliza el algoritmo de cifrado AES-256 de código estándar para cifrar los datos en el servidor que aloja la instancia de base de datos de RDS. Una vez cifrados los datos, Amazon RDS se encarga de la autenticación de acceso y del descifrado de los datos de forma transparente, con un impacto mínimo en el desempeño. No es necesario modificar las aplicaciones cliente de base de datos para utilizar el cifrado.

El cifrado de Amazon RDS actualmente está disponible para todos los motores de bases de datos y tipos de almacenamiento. El cifrado de Amazon RDS está disponible para la mayoría de las clases de instancias de bases de datos. Para obtener información acerca de las clases de instancia de base de datos que no admiten el cifrado de Amazon RDS, consulte [Cifrado de recursos de Amazon RDS](#) en la Guía del usuario de Amazon RDS.

Corrección

Para obtener información sobre el cifrado de instancias de base de datos en Amazon RDS, consulte [Cifrar los recursos de Amazon RDS](#) en la Guía del usuario de Amazon RDS.

Las instantáneas de clústeres y bases de datos de RDS [RDS.4] deben cifrarse cuando están inactivas

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::RDS::DBClusterSnapshot, AWS::RDS::DBSnapshot

Regla de AWS Config : [rds-snapshot-encrypted](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instantánea de base de datos de RDS está cifrada. El control falla si una instantánea de base de datos de RDS no está cifrada.

Este control está diseñado para instancias de base de datos de RDS. Sin embargo, también puede generar resultados para instantáneas de instancias de base de datos de Aurora, instancias de base de datos de Neptune y clústeres de Amazon DocumentDB. Si estos resultados no son útiles, puede suprimirlos.

El cifrado de los datos en reposo reduce el riesgo de que un usuario no autenticado acceda a los datos almacenados en el disco. Los datos de las instantáneas de RDS deben cifrarse en reposo para ofrecer un nivel de seguridad adicional.

Corrección

Para cifrar una instantánea de RDS, consulte [Cifrar los recursos de Amazon RDS](#) en la Guía del usuario de Amazon RDS. Cuando cifra una instancia de base de datos de RDS, los datos cifrados incluyen el almacenamiento subyacente de la instancia, sus copias de seguridad automatizadas, sus réplicas de lectura y sus instantáneas.

Solo se puede cifrar una instancia de base de datos de RDS al crearla, no después de que se haya creado. Sin embargo, debido a que se puede cifrar una copia de una instantánea de base de datos sin cifrar, en la práctica es posible agregar el cifrado a una instancia de base de datos sin cifrar. Es decir, puede crear una instantánea de una instancia de base de datos y, a continuación, crear una

copia cifrada de esa instantánea. A continuación, se puede restaurar una instancia de base de datos a partir de la instantánea cifrada y de este modo, se tiene una copia cifrada de la instancia de base de datos original.

Las instancias de base de datos de RDS [RDS.5] deben configurarse con varias zonas de disponibilidad

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [rds-multi-az-support](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la alta disponibilidad está habilitada para sus instancias de base de datos de RDS. El control falla si una instancia de base de datos de RDS no está configurada con varias zonas de disponibilidad (). AZs Este control no se aplica a las instancias de base de datos de RDS que forman parte de una implementación de un clúster de base de datos Multi-AZ.

La configuración de las instancias de base de datos de Amazon RDS AZs ayuda a garantizar la disponibilidad de los datos almacenados. Las implementaciones en zonas de disponibilidad múltiples permiten la conmutación por error automática si hay algún problema con la disponibilidad de las zonas de disponibilidad y durante el mantenimiento regular del RDS.

Corrección

Para implementar sus instancias de base de datos en varias instancias AZs, [modifique una instancia de base de datos para que sea una implementación de instancia de base de datos Multi-AZ](#) en la Guía del usuario de Amazon RDS.

Se debe configurar una supervisión mejorada para las instancias de base de datos de RDS [RDS.6]

Requisitos relacionados: NIST.800-53.r5 NIST.800-53.r5 CA-7 SI-2

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [rds-enhanced-monitoring-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub	
monitoringInterval	Número de segundos entre los intervalos de recopilación de métricas de supervisión	Enum	1, 5, 10, 15, 30, 60	Sin valor predeterminado	

Este control comprueba si la supervisión mejorada está habilitada para una instancia de base de datos de Amazon Relational Database Service (Amazon RDS). Se produce un error en el control si la supervisión mejorada no está habilitada para la instancia. Si proporciona un valor personalizado para el parámetro `monitoringInterval`, el control pasa si se recopilan métricas de supervisión mejoradas para la instancia en el intervalo especificado.

En Amazon RDS, la supervisión mejorada permite una respuesta más rápida a los cambios de rendimiento en la infraestructura subyacente. Estos cambios en el rendimiento podrían provocar una falta de disponibilidad de los datos. El monitoreo mejorado proporciona métricas en tiempo real para el sistema operativo en el que se ejecuta la instancia de base de datos de RDS. El agente está instalado en la instancia. El agente puede obtener métricas con mayor precisión de lo que es posible desde la capa del hipervisor.

Las métricas de monitorización mejoradas son útiles cuando desea ver cómo diferentes procesos o subprocesos en una instancia de base de datos usan la CPU. Para obtener más información, consulte [Enhanced Monitoring](#) (Supervisión mejorada) en la Guía del usuario de Amazon RDS.

Corrección

Para obtener instrucciones detalladas sobre cómo habilitar la supervisión mejorada para su instancia de base de datos, consulte [Configuración y activación de la supervisión mejorada](#) en la Guía del usuario de Amazon RDS.

Los clústeres de RDS [RDS.7] deben tener habilitada la protección contra la eliminación

Requisitos relacionados: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Gravedad: baja

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [rds-cluster-deletion-protection-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos RDS tiene habilitada la protección contra eliminación. El control falla si un clúster de base de datos RDS no tiene habilitada la protección contra eliminación.

Este control está diseñado para instancias de base de datos de RDS. Sin embargo, también puede generar resultados para instancias de base de datos de Aurora, instancias de base de datos de Neptune y clústeres de Amazon DocumentDB. Si estos resultados no son útiles, puede suprimirlos.

Habilitar la protección contra la eliminación de clústeres es un nivel adicional de protección contra la eliminación accidental de la base de datos o la eliminación por parte de una entidad no autorizada.

Cuando la protección de eliminación está habilitada, no se puede eliminar un clúster de base de datos. Para que una solicitud de eliminación se pueda realizar correctamente, la protección contra la eliminación debe estar deshabilitada.

Corrección

Para habilitar la protección contra la eliminación de un clúster de base de datos de RDS, consulte [Modificación del clúster de base de datos mediante la consola, la CLI y la API](#) en la Guía del usuario de Amazon RDS. En Protección contra eliminación, elija Habilitar la protección contra eliminación.

Las instancias de base de datos de RDS [RDS.8] deben tener habilitada la protección contra la eliminación

Requisitos relacionados: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Gravedad: baja

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [rds-instance-deletion-protection-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros:

- databaseEngines: mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web (no personalizable)

Este control comprueba si las instancias de base de datos de RDS que utilizan uno de los motores de bases de datos de la lista tienen habilitada la protección contra la eliminación. El control falla si una instancia de base de datos RDS no tiene habilitada la protección contra eliminación.

La activación de la protección contra la eliminación de instancias es un nivel adicional de protección contra la eliminación accidental de la base de datos o la eliminación por parte de una entidad no autorizada.

Mientras la protección contra la eliminación está habilitada, no se puede eliminar una instancia de base de datos de RDS. Para que una solicitud de eliminación se pueda realizar correctamente, la protección contra la eliminación debe estar deshabilitada.

Corrección

Para habilitar la protección contra la eliminación de una instancia de base de datos de RDS, consulte [Modificación de una instancia de base de datos de Amazon RDS](#) en la Guía del usuario de Amazon RDS. En Protección contra eliminación, elija Habilitar la protección contra eliminación.

[RDS.9] Las instancias de base de datos de RDS deben publicar los registros en Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), (10), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 Nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.r5 SI-4 (20), Nist.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [rds-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instancia de base de datos de Amazon RDS está configurada para publicar los siguientes registros en Amazon CloudWatch Logs. El control falla si la instancia no está configurada para publicar los siguientes registros en CloudWatch Logs:

- Oracle: alerta, auditoría, rastreo, escucha
- PostgreSQL: Postgresql, actualización
- MySQL: Auditoría, Error, General, SlowQuery
- MariaDB: Auditoría, Error, General, SlowQuery
- SQL Server: error, agente
- Aurora: auditoría, error, general, SlowQuery
- Aurora-MySQL: Auditoría, Error, General, SlowQuery
- Aurora-PostgreSQL: PostgreSQL

Las bases de datos de RDS deben tener habilitados los registros relevantes. El registro de la base de datos proporciona registros detallados de las solicitudes realizadas a RDS. Los registros de las bases de datos pueden ayudar con las auditorías de seguridad y acceso y pueden ayudar a diagnosticar problemas de disponibilidad.

Corrección

Para obtener información sobre la publicación de registros de bases de datos de RDS en CloudWatch Logs, consulte [Especificar los registros que se van a publicar en CloudWatch Logs](#) en la Guía del usuario de Amazon RDS.

La autenticación de IAM [RDS.10] debe configurarse para las instancias de RDS

Requisitos relacionados: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Categoría: Proteger > Gestión del acceso seguro > Autenticación sin contraseña

Gravedad: media

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [rds-instance-iam-authentication-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instancia de base de datos de RDS tiene habilitada la autenticación de bases de datos de IAM. El control falla si la autenticación de IAM no está configurada para las instancias de base de datos de RDS. Este control solo evalúa las instancias de RDS con los siguientes tipos de motor: mysql, postgres, aurora, aurora-mysql, aurora-postgresql y mariadb. Una instancia de RDS también debe estar en uno de los siguientes estados para que se genere un resultado: available, backing-up, storage-optimization o storage-full.

La autenticación de bases de datos de IAM permite autenticar las instancias de bases de datos con un token de autenticación en lugar de una contraseña. El tráfico de red hacia y desde la base de datos se cifra mediante SSL. Para obtener más información, consulte [Autenticación de bases de datos de IAM](#) en la Guía del usuario de Amazon Aurora.

Corrección

Para activar la autenticación de bases de datos de IAM en una instancia de base de datos de RDS, consulte [Habilitar y deshabilitar la autenticación de bases de datos de IAM](#) en la Guía del usuario de Amazon RDS.

Las instancias RDS [RDS.11] deben tener habilitadas las copias de seguridad automáticas

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: media

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [db-instance-backup-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
backupRetentionMinimum	El periodo mínimo de retención de copias de seguridad en días	Entero	De 7 a 35	7
checkReadReplicas	Comprueba si las instancias de base de datos de RDS tienen habilitadas las copias de seguridad para las réplicas de lectura	Booleano	No personalizable	false

Este control comprueba si la instancia de Amazon Relational Database Service tiene habilitadas las copias de seguridad automáticas y si el periodo de retención de las copias de seguridad es superior

o igual al periodo especificado. Las réplicas de lectura se excluyen de la evaluación. Se produce un error en el control si las copias de seguridad no están habilitadas para la instancia o si el periodo de retención es inferior al periodo especificado. A menos que se proporcione un valor personalizado de parámetro para el periodo de retención de copia de seguridad, Security Hub utiliza un valor predeterminado de 7 días.

Las copias de seguridad le ayudan a recuperarse más rápidamente de un incidente de seguridad y refuerzan la resiliencia de sus sistemas. Amazon RDS permite configurar instantáneas diarias del volumen de instancias completo. Para más información sobre las copias de seguridad automatizadas de Amazon RDS, consulte [Trabajo con copias de seguridad](#) en la Guía del usuario de Amazon RDS.

Corrección

Para habilitar copias de seguridad automatizadas para una instancia de base de datos de RDS, consulte [Habilitación de copias de seguridad automatizadas](#) en Guía del usuario de Amazon RDS.

La autenticación de IAM [RDS.12] debe configurarse para los clústeres de RDS

Requisitos relacionados: (1), (15), (7), NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6

Categoría: Proteger > Gestión del acceso seguro > Autenticación sin contraseña

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [rds-cluster-iam-authentication-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de Amazon RDS tiene habilitada la autenticación de bases de datos de IAM.

La autenticación de bases de datos de IAM permite autenticar las instancias de bases de datos sin contraseña. La autenticación usa un token de autenticación. El tráfico de red hacia y desde la base de datos se cifra mediante SSL. Para obtener más información, consulte [Autenticación de bases de datos de IAM](#) en la Guía del usuario de Amazon Aurora.

Corrección

Para habilitar la autenticación de IAM para un clúster de base de datos, consulte [Habilitar y deshabilitar la autenticación de bases de datos de IAM](#) en la Guía del usuario de Amazon Aurora.

Las actualizaciones automáticas de las versiones secundarias de RDS [RDS.13] deben estar habilitadas

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.3.2, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: alta

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [rds-automatic-minor-version-upgrade-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las actualizaciones automáticas de las versiones secundarias están habilitadas para la instancia de base de datos de RDS.

Las actualizaciones automáticas de las versiones secundarias actualizan periódicamente una base de datos a las versiones recientes del motor de base de datos. Sin embargo, es posible que la actualización no siempre incluya la versión más reciente del motor de base de datos. Si necesita mantener las bases de datos en versiones específicas en momentos determinados, le recomendamos que las actualice manualmente a las versiones de base de datos que necesite según el calendario requerido. En caso de problemas de seguridad críticos o cuando una versión alcance su end-of-support fecha límite, Amazon RDS podría aplicar una actualización de la versión secundaria aunque no haya activado la opción de actualización automática de la versión secundaria. Para obtener más información, consulte la documentación de actualización de Amazon RDS para su motor de base de datos específico:

- [Actualizaciones automáticas de versiones secundarias de RDS para MariaDB](#)
- [Actualizaciones automáticas de versiones secundarias de RDS for MySQL](#)
- [Actualizaciones automáticas de versiones secundarias de RDS para PostgreSQL](#)
- [Versiones de Db2 en Amazon RDS](#)

- [Actualizaciones de versiones secundarias de Oracle](#)
- [Actualizaciones del motor de base de datos de Microsoft SQL Server](#)

Corrección

Para habilitar las actualizaciones automáticas de las versiones secundarias de una instancia de base de datos existente, consulte [Modificación de una instancia de base de datos de Amazon RDS](#) en la Guía del usuario de Amazon RDS. Para la actualización automática de una versión secundaria, seleccione Sí.

Los clústeres de Amazon Aurora [RDS.14] deben tener habilitada la característica de búsqueda de datos anteriores

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SI-13(5)

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [aurora-mysql-backtracking-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub	
BacktrackWindowInHours	Número de horas necesarias para hacer búsquedas de datos anteriores en un clúster Aurora MySQL	Doble	De 0.1 a 72	Sin valor predeterminado	

Este control comprueba si un clúster de Amazon Aurora tiene habilitada la característica de búsqueda de datos anteriores. Se produce un error en el control si el clúster no tiene habilitada la búsqueda de datos anteriores. Si proporciona un valor personalizado para el parámetro `BacktrackWindowInHours`, el control solo pasa si la búsqueda de datos anteriores en el clúster se hace durante el periodo especificado.

Las copias de seguridad le ayudan a recuperarse más rápidamente de un incidente de seguridad. También refuerzan la resiliencia de sus sistemas. La búsqueda de datos anteriores de Aurora reduce el tiempo de recuperación de una base de datos en un punto en el tiempo. Para ello, no es necesario restaurar la base de datos.

Corrección

Para habilitar la búsqueda de datos anteriores de Aurora, consulte [Configuración de la búsqueda de datos anteriores](#) en la Guía del usuario de Amazon Aurora.

Tenga en cuenta que no puede habilitar la búsqueda de datos anteriores en un clúster existente. En su lugar, puede crear un clon que tenga habilitado la búsqueda de datos anteriores. Para obtener más información sobre las limitaciones de la búsqueda de datos anteriores de Aurora, consulte la lista de limitaciones en [Descripción general de búsqueda de datos anteriores](#).

Los clústeres de bases de datos de RDS [RDS.15] deben configurarse para varias zonas de disponibilidad

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 SC-3 6, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [rds-cluster-multi-az-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la alta disponibilidad está habilitada para sus clústeres de base de datos de RDS. El control falla si un clúster de base de datos de RDS no está implementado en varias zonas de disponibilidad (). AZs

Los clústeres de bases de datos de RDS deben configurarse para varios AZs a fin de garantizar la disponibilidad de los datos almacenados. La implementación en varias zonas AZs permite la conmutación por error automática en caso de que se produzca un problema de disponibilidad en las zonas de disponibilidad y durante los eventos de mantenimiento habituales del RDS.

Corrección

Para implementar sus clústeres de base de datos en varios AZs, [modifique una instancia de base de datos para que sea un despliegue de instancias de base de datos Multi-AZ](#) en la Guía del usuario de Amazon RDS.

Los pasos de solución son diferentes para las bases de datos globales de Aurora. Para configurar varias zonas de disponibilidad para una base de datos global de Aurora, seleccione su clúster de base de datos. A continuación, elija Acciones y Añadir lector, y especifique varios. AZs Para obtener más información, consulte [Agregar réplicas Aurora a un clúster de base de datos](#) en la Guía del usuario de Amazon Aurora.

Los clústeres de bases de datos de RDS [RDS.16] deben configurarse para copiar etiquetas en las instantáneas

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), Nist.800-53.r5 CM-2, Nist.800-53.r5 CM-2 (2)

Categoría: Identificar - Inventario

Gravedad: baja

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : `rds-cluster-copy-tags-to-snapshots-enabled` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los clústeres de bases de datos de RDS están configurados para copiar todas las etiquetas en las instantáneas cuando se crean las instantáneas.

La identificación y el inventario de sus activos de TI es un aspecto fundamental de seguridad y control. Tiene que tener una visión de todos sus clústeres de base de datos de RDS para que pueda evaluar sus posiciones de seguridad y tomar así las acciones pertinentes respecto a las posibles áreas débiles. Las instantáneas deben etiquetarse de la misma manera que sus clústeres de bases

de datos de RDS principales. Al habilitar esta configuración, se garantiza que las instantáneas hereden las etiquetas de sus clústeres de bases de datos principales.

Corrección

Para copiar automáticamente las etiquetas en las instantáneas de un clúster de base de datos de RDS, consulte [Modificación del clúster de base de datos mediante la consola, la CLI y la API](#) en la Guía del usuario de Amazon Aurora. Seleccione Copiar etiquetas en instantáneas

Las instancias de base de datos de RDS [RDS.17] deben configurarse para copiar etiquetas en las instantáneas

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NiSt.800-53.r5 CM-2, NiSt.800-53.r5 CM-2 (2)

Categoría: Identificar - Inventario

Gravedad: baja

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : `rds-instance-copy-tags-to-snapshots-enabled` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las instancias de base de datos de RDS están configuradas para copiar todas las etiquetas a las instantáneas cuando se crean las instantáneas.

La identificación y el inventario de sus activos de TI es un aspecto fundamental de seguridad y control. Tiene que tener una visión de todas sus instancias de base de datos de RDS para que pueda evaluar sus posiciones de seguridad y tomar así las acciones pertinentes respecto a las posibles áreas débiles. Las instantáneas se deben etiquetar de la misma manera que las instancias de base de datos RDS principales. Al habilitar esta configuración, se garantiza que las instantáneas hereden las etiquetas de sus instancias de base de datos principales.

Corrección

Para copiar automáticamente las etiquetas en las instantáneas de una instancia de base de datos de RDS, consulte [Modificación de una instancia de base de datos de Amazon RDS](#) en la Guía del usuario de Amazon RDS. Seleccione Copiar etiquetas en instantáneas

Las instancias de RDS [RDS.18] deben implementarse en una VPC

Categoría: Proteger > Configuración de red segura > Recursos dentro de VPC

Gravedad: alta

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : rds-deployed-in-vpc (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instancia de Amazon RDS está implementada en una EC2 -VPC.

VPCs proporcionan una serie de controles de red para proteger el acceso a los recursos de RDS. Estos controles incluyen puntos finales de VPC ACLs, redes y grupos de seguridad. Para aprovechar estos controles, le recomendamos que cree las instancias de RDS en una EC2 -VPC.

Corrección

Para obtener instrucciones sobre cómo mover instancias de RDS a una VPC, consulte [Actualización de la VPC de una instancia de base de datos](#) en la Guía del usuario de Amazon RDS.

Las suscripciones de notificación de eventos de RDS [RDS.19] existentes deben configurarse para los eventos de clúster críticos

Requisitos relacionados: NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2

Categoría: Detectar > Servicios de detección > Supervisión de aplicaciones

Gravedad: baja

Tipo de recurso: AWS::RDS::EventSubscription

Regla de AWS Config : rds-cluster-event-notifications-configured (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una suscripción a eventos de Amazon RDS existente para clústeres de base de datos tiene habilitadas notificaciones para los siguientes pares clave-valor de tipo de origen y categoría de evento:

```
DBCluster: ["maintenance","failure"]
```

El control se transfiere si no hay suscripciones a eventos existentes en su cuenta.

Las notificaciones de eventos de RDS utilizan Amazon SNS para informarle de los cambios en la disponibilidad o la configuración de sus recursos de RDS. Estas notificaciones permiten una respuesta rápida. Para obtener más información sobre las notificaciones de eventos de RDS, consulte [Uso de las notificaciones de eventos de Amazon RDS](#) en la Guía del usuario de Amazon RDS.

Corrección

Para suscribirse a las notificaciones de eventos del clúster de RDS, consulte [Suscribirse a las notificaciones de eventos de Amazon RDS](#) en la Guía del usuario de Amazon RDS. Use los siguientes valores:

Campo	Valor
Tipo de origen	Clústeres
Clústeres que se van a incluir	Todos los clústeres
Categorías de eventos a incluir	Seleccione categorías de eventos específicas o Todas las categorías de eventos

Las suscripciones de notificación de eventos de RDS [RDS.20] existentes deben configurarse para eventos críticos de instancias de bases de datos

Requisitos relacionados: NIST.800-53.r5 SI-2, PCI DSS v4.0.1/11.5.2 NIST.800-53.r5 CA-7

Categoría: Detectar > Servicios de detección > Supervisión de aplicaciones

Gravedad: baja

Tipo de recurso: AWS::RDS::EventSubscription

Regla de AWS Config : `rds-instance-event-notifications-configured` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una suscripción a eventos de Amazon RDS existente para instancias de base de datos tiene habilitadas notificaciones para los siguientes pares clave-valor de tipo de origen y categoría de evento:

```
DBInstance: ["maintenance","configuration change","failure"]
```

El control se transfiere si no hay suscripciones a eventos existentes en su cuenta.

Las notificaciones de eventos de RDS utilizan Amazon SNS para informarle de los cambios en la disponibilidad o la configuración de sus recursos de RDS. Estas notificaciones permiten una respuesta rápida. Para obtener más información sobre las notificaciones de eventos de RDS, consulte [Uso de las notificaciones de eventos de Amazon RDS](#) en la Guía del usuario de Amazon RDS.

Corrección

Para suscribirse a las notificaciones de eventos de instancias de RDS, consulte [Suscribirse a las notificaciones de eventos de Amazon RDS](#) en la Guía del usuario de Amazon RDS. Use los siguientes valores:

Campo	Valor
Tipo de origen	instancias
Instancias que se van a incluir	Todas las instancias
Categorías de eventos a incluir	Seleccione categorías de eventos específicas o Todas las categorías de eventos

Se debe configurar una suscripción a las notificaciones de eventos de RDS [RDS.21] para los eventos críticos de los grupos de parámetros de bases de datos

Requisitos relacionados: NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, PCI DSS v4.0.1/11.5.2

Categoría: Detectar > Servicios de detección > Supervisión de aplicaciones

Gravedad: baja

Tipo de recurso: AWS::RDS::EventSubscription

Regla de AWS Config : rds-pg-event-notifications-configured (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si existe una suscripción a eventos de Amazon RDS con notificaciones habilitadas para los siguientes pares clave-valor de tipo de fuente y categoría de evento. El control se transfiere si no hay suscripciones a eventos existentes en su cuenta.

```
DBParameterGroup: ["configuration change"]
```

Las notificaciones de eventos de RDS utilizan Amazon SNS para informarle de los cambios en la disponibilidad o la configuración de sus recursos de RDS. Estas notificaciones permiten una respuesta rápida. Para obtener más información sobre las notificaciones de eventos de RDS, consulte [Uso de las notificaciones de eventos de Amazon RDS](#) en la Guía del usuario de Amazon RDS.

Corrección

Para suscribirse a las notificaciones de eventos del grupo de parámetros de la base de datos de RDS, consulte [Suscripción a la notificación de eventos de Amazon RDS](#) en la Guía del usuario de Amazon RDS. Use los siguientes valores:

Campo	Valor
Tipo de origen	Grupos de parámetros
Grupos de parámetros que se van a incluir	Todos los grupos de parámetros
Categorías de eventos a incluir	Seleccione categorías de eventos específicas o Todas las categorías de eventos

Se debe configurar una suscripción a las notificaciones de eventos de RDS [RDS.22] para los eventos críticos de los grupos de seguridad de bases de datos

Requisitos relacionados: NIST.800-53.r5 CA-7 NIST.800-53.r5 SI-2, PCI DSS v4.0.1/11.5.2

Categoría: Detectar > Servicios de detección > Supervisión de aplicaciones

Gravedad: baja

Tipo de recurso: AWS::RDS::EventSubscription

Regla de AWS Config : rds-sg-event-notifications-configured (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si existe una suscripción a eventos de Amazon RDS con notificaciones habilitadas para los siguientes pares clave-valor de tipo de fuente y categoría de evento. El control se transfiere si no hay suscripciones a eventos existentes en su cuenta.

```
DBSecurityGroup: ["configuration change","failure"]
```

Las notificaciones de eventos de RDS utilizan Amazon SNS para informarle de los cambios en la disponibilidad o la configuración de sus recursos de RDS. Estas notificaciones permiten una respuesta rápida. Para obtener más información sobre las notificaciones de eventos de RDS, consulte [Uso de las notificaciones de eventos de Amazon RDS](#) en la Guía del usuario de Amazon RDS.

Corrección

Para suscribirse a las notificaciones de eventos de instancias de RDS, consulte [Suscribirse a las notificaciones de eventos de Amazon RDS](#) en la Guía del usuario de Amazon RDS. Use los siguientes valores:

Campo	Valor
Tipo de origen	Grupos de seguridad

Campo	Valor
Grupos de seguridad que se van a incluir	Todos los grupos de seguridad
Categorías de eventos a incluir	Seleccione categorías de eventos específicas o Todas las categorías de eventos

Las instancias RDS [RDS.23] no deben usar el puerto predeterminado de un motor de base de datos

Requisitos relacionados: (21) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (16), (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: baja

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : rds-no-default-ports (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster o instancia de RDS utiliza un puerto distinto del puerto predeterminado del motor de base de datos. El control falla si el clúster o la instancia de RDS utilizan el puerto predeterminado. Este control no se aplica a las instancias de RDS que forman parte de un clúster.

Si utiliza un puerto conocido para implementar un clúster o una instancia de RDS, un atacante puede adivinar la información sobre el clúster o la instancia. El atacante puede usar esta información junto con otra información para conectarse a un clúster o instancia de RDS u obtener información adicional sobre la aplicación.

Al cambiar el puerto, también debe actualizar las cadenas de conexión existentes que se utilizaron para conectarse al puerto anterior. También debe comprobar el grupo de seguridad de la instancia de base de datos para asegurarse de que incluye una regla de entrada que permita la conectividad en el nuevo puerto.

Corrección

Para modificar el puerto predeterminado de una instancia de base de datos de RDS existente, consulte [Modificación de una instancia de base de datos de Amazon RDS](#) en la Guía del usuario de Amazon RDS. Para modificar el puerto predeterminado de un clúster de base de datos de RDS existente, consulte [Modificación del clúster de base de datos mediante la consola, la CLI y la API](#) en la Guía del usuario de Amazon Aurora. Para el Puerto de base de datos, cambie el valor del puerto por un valor que no sea el predeterminado.

Los clústeres de bases de datos de RDS [RDS.24] deben usar un nombre de usuario de administrador personalizado

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, PCI DSS v4.0.1/2.2.2

Categoría: Identificar > Configuración de recursos

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

Regla de AWS Config : [rds-cluster-default-admin-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de Amazon RDS ha cambiado el nombre de usuario de administrador con respecto a su valor predeterminado. El control no se aplica a los motores del tipo neptune (Neptune DB) o docdb (DocumentDB). Esta regla fallará si el nombre de usuario del administrador está establecido en el valor predeterminado.

Al crear una base de datos de Amazon RDS, debe cambiar el nombre de usuario de administrador predeterminado por un valor único. Los nombres de usuario predeterminados son de dominio público y deben cambiarse durante la creación de la base de datos de RDS. Cambiar los nombres de usuario predeterminados reduce el riesgo de accesos no deseados.

Corrección

Para cambiar el nombre de usuario de administrador asociado al clúster de base de datos de Amazon RDS, [cree un nuevo clúster de base de datos de RDS](#) y cambie el nombre de usuario de administrador predeterminado al crear la base de datos.

Las instancias de bases de datos de RDS [RDS.25] deben usar un nombre de usuario de administrador personalizado

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, PCI DSS v4.0.1/2.2.2

Categoría: Identificar > Configuración de recursos

Gravedad: media

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [rds-instance-default-admin-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si ha cambiado el nombre de usuario administrativo de las instancias de base de datos de Amazon Relational Database Service (Amazon RDS) con respecto al valor predeterminado. El control falla si el nombre de usuario administrativo está establecido en el valor predeterminado. El control no se aplica a los motores del tipo neptune (Neptune DB) o docdb (DocumentDB) ni a las instancias de RDS que forman parte de un clúster.

Los nombres de usuario administrativos predeterminados en las bases de datos de Amazon RDS son de dominio público. Al crear una base de datos de Amazon RDS, debe cambiar el nombre de usuario administrativo predeterminado por un valor único para reducir el riesgo de accesos no deseados.

Corrección

Para cambiar el nombre de usuario administrativo asociado a una instancia de base de datos de RDS, [cree primero una nueva instancia de base de datos de RDS](#). Cambie el nombre de usuario administrativo predeterminado al crear la base de datos.

Las instancias de base de datos de RDS [RDS.26] deben protegerse mediante un plan de copias de seguridad

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Gravedad: media

Tipo de recurso: AWS::RDS::DBInstance

AWS Config regla: [rds-resources-protected-by-backup-plan](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
backupVaultLockCheck	El control produce un PASSED resultado si el parámetro está establecido en true y el recurso utiliza AWS Backup Vault Lock.	Booleano	true o false	Sin valor predeterminado

Este control evalúa si las instancias de base de datos de Amazon RDS están cubiertas por un plan de copias de seguridad. Se produce un error en este control si la instancia de base de datos de RDS no está cubierta por un plan de copias de seguridad. Si establece el backupVaultLockCheck parámetro en un valor igual a true, el control solo se activará si la instancia está guardada en un almacén AWS Backup cerrado con llave.

AWS Backup es un servicio de copias de seguridad totalmente gestionado que centraliza y automatiza las copias de seguridad de todos los datos. Servicios de AWS Con él AWS Backup, puede crear políticas de respaldo denominadas planes de respaldo. Puede utilizar estos planes para definir los requisitos de copia de seguridad, como la frecuencia con la que se va a realizar la copia de seguridad de los datos y el tiempo durante el que se van a conservar esas copias de seguridad. La inclusión de instancias de base de datos de RDS en un plan de copias de seguridad le ayuda a proteger sus datos contra pérdidas o eliminaciones involuntarias.

Corrección

Para añadir una instancia de base de datos de RDS a un plan de AWS Backup respaldo, consulte [Asignación de recursos a un plan de respaldo](#) en la Guía para AWS Backup desarrolladores.

Los clústeres de bases de datos de RDS [RDS.27] deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

AWS Config regla: [rds-cluster-encrypted-at-rest](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos de RDS está cifrado en reposo. El control falla si un clúster de base de datos de RDS no está cifrado en reposo.

Los datos en reposo se refieren a cualquier dato que se almacene en un almacenamiento persistente y no volátil durante cualquier período de tiempo. El cifrado le ayuda a proteger la confidencialidad de dichos datos, reduciendo el riesgo de que un usuario no autorizado pueda acceder a ellos. El cifrado de los clústeres de bases de datos de RDS protege sus datos y metadatos contra el acceso no autorizado. También cumple con los requisitos de conformidad para el data-at-rest cifrado de los sistemas de archivos de producción.

Corrección

Puede habilitar el cifrado en reposo al crear un clúster de base de datos de RDS. No se puede cambiar la configuración de cifrado después de crear un clúster. Para obtener más información, consulte [Cifrado de un clúster de base de datos de Amazon Aurora](#) en la Guía del usuario de Amazon Aurora.

[RDS.28] Los clústeres de base de datos de RDS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBCluster`

AWS Config regla: `tagged-rds-dbccluster` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un clúster de base de datos de Amazon RDS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el clúster de base de datos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el clúster de base de datos no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS

los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un clúster de base de datos de RDS, consulte [Etiquetado de los recursos de Amazon RDS](#) en la Guía del usuario de Amazon RDS.

[RDS.29] Las instantáneas del clúster de base de datos de RDS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::RDS::DBClusterSnapshot

AWS Config regla: tagged-rds-dbcustersnapshot (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.		que cumplan con AWS los requisitos .	

Este control comprueba si una instantánea de clúster de base de datos de Amazon RDS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la instantánea de clúster de base de datos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la instantánea de clúster de base de datos no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws :`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a la instantánea de clúster de base de datos de RDS, consulte [Etiquetado de los recursos de Amazon RDS](#) en la Guía del usuario de Amazon RDS.

[RDS.30] Las instancias de bases de datos de RDS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::RDS::DBInstance

AWS Config regla: tagged-rds-dbinstance (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una instancia de base de datos de Amazon RDS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la instancia de base de datos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la instancia de base de datos no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una instancia de base de datos de RDS, consulte [Etiquetado de los recursos de Amazon RDS](#) en la Guía del usuario de Amazon RDS.

[RDS.31] Los grupos de seguridad de bases de datos de RDS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::RDS::DBSecurityGroup

AWS Config regla: tagged-rds-dbsecuritygroup (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un grupo de seguridad de base de datos de Amazon RDS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el grupo de seguridad de base de datos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el grupo de seguridad de base de datos no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre

ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un grupo de seguridad de base de datos de RDS, consulte [Etiquetado de los recursos de Amazon RDS](#) en la Guía del usuario de Amazon RDS.

[RDS.32] Las instantáneas de bases de datos de RDS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS : :RDS : :DBSnapshot

AWS Config regla: tagged-rds-dbsnapshot (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una instantánea de base de datos de Amazon RDS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la instantánea de base de datos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un

error si la instantánea de base de datos no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws :`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar una instantánea de base de datos de RDS, consulte [Etiquetado de los recursos de Amazon RDS](#) en la Guía del usuario de Amazon RDS.

[RDS.33] Los grupos de subredes de bases de datos de RDS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::RDS::DBSubnetGroup`

AWS Config regla: `tagged-rds-dbsubnetgroups` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un grupo de subredes de bases de datos de Amazon RDS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el grupo de subredes de bases de datos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el grupo de subredes de bases de datos no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre

ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un grupo de subredes de bases de datos de RDS, consulte [Etiquetado de los recursos de Amazon RDS](#) en la Guía del usuario de Amazon RDS.

[RDS.34] Los clústeres de bases de datos Aurora MySQL deberían publicar los registros de auditoría en Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), Nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.r5 SI-4 (20), Nist.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.2.1 NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

AWS Config regla: [rds-aurora-mysql-audit-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos Amazon Aurora MySQL está configurado para publicar registros de auditoría en Amazon CloudWatch Logs. El control falla si el clúster no está configurado para publicar los registros de auditoría en CloudWatch Logs. El control no genera resultados para los clústeres de base de datos Aurora sin servidor v1.

Los registros de auditoría recopilan un registro de la actividad de la base de datos, incluidos los intentos de inicio de sesión, las modificaciones de datos, los cambios de esquema y otros eventos que se pueden auditar por motivos de seguridad y conformidad. Al configurar un clúster de base de datos Aurora MySQL para publicar registros de auditoría en un grupo de CloudWatch registros de Amazon Logs, puede realizar un análisis en tiempo real de los datos de registro. CloudWatch Logs conserva los registros en un almacenamiento de alta duración. También puede crear alarmas y ver las métricas en CloudWatch.

 Note

Una forma alternativa de publicar los registros de auditoría en CloudWatch Logs consiste en habilitar la auditoría avanzada y configurar el parámetro de base de datos a nivel de clúster en. `server_audit_logs_upload` 1 El valor predeterminado de `server_audit_logs_upload` parameter es 0. Sin embargo, le recomendamos que utilice las siguientes instrucciones de corrección para pasar este control.

Corrección

Para publicar los registros de auditoría del clúster de base de datos Aurora MySQL en CloudWatch Logs, consulte [Publicar registros de Amazon Aurora MySQL en Amazon CloudWatch Logs](#) en la Guía del usuario de Amazon Aurora.

Los clústeres de bases de datos de RDS [RDS.35] deben tener habilitada la actualización automática de las versiones secundarias

Requisitos relacionados: NIST.800-53.r5 SI-2, niST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0.1/6.3.3

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: media

Tipo de recurso: AWS::RDS::DBCluster

AWS Config regla: [rds-cluster-auto-minor-version-upgrade-enable](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la actualización automática de la versión secundaria está habilitada para un clúster de base de datos de Amazon RDS Multi-AZ. El control lanza un error si la actualización automática de la versión secundaria no está habilitada para un clúster de base de datos en varias zonas de disponibilidad.

RDS proporciona la actualización automática de las versiones secundarias para que pueda mantener actualizado el clúster de base de datos en varias zonas de disponibilidad. Las versiones secundarias pueden introducir nuevas funciones de software, correcciones de errores, parches de seguridad y

mejoras de rendimiento. Al habilitar la actualización automática de las versiones secundarias en los clústeres de bases de datos de RDS, el clúster, junto con las instancias del clúster, recibirá actualizaciones automáticas de la versión secundaria cuando haya nuevas versiones disponibles. Las actualizaciones se aplican automáticamente durante el período de mantenimiento.

Corrección

Para habilitar la actualización automática de las versiones secundarias en clústeres de bases de datos en varias zonas de disponibilidad, consulte [Modificación de un clúster de base de datos Multi-AZ](#) en la Guía del usuario de Amazon RDS.

[RDS.36] Las instancias de base de datos de RDS para PostgreSQL deben publicar registros en Logs CloudWatch

Requisitos relacionados: PCI DSS v4.0.1/10.4.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [rds-postgresql-logs-to-cloudwatch](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
logTypes	Lista de tipos de registros separados por comas que se publicarán en Logs CloudWatch	StringList	No personalizable	postgresql

Este control comprueba si una instancia de base de datos de Amazon RDS for PostgreSQL está configurada para publicar registros en Amazon Logs. CloudWatch El control falla si la instancia de

base de datos PostgreSQL no está configurada para publicar los tipos de registro mencionados en `logTypes` el parámetro en `Logs`. `CloudWatch`

El registro de base de datos proporciona detalles sobre las solicitudes realizadas a una instancia de RDS. PostgreSQL genera registros de eventos que contienen información útil para los administradores. La publicación de estos registros en `CloudWatch Logs` centraliza la administración de registros y le ayuda a realizar análisis en tiempo real de los datos de registro. `CloudWatch Logs` retiene los registros en un almacenamiento muy duradero. También puede crear alarmas y ver las métricas en `CloudWatch`.

Corrección

Para publicar registros de instancias de base de datos de PostgreSQL en `Logs`, consulte `CloudWatch` [Publicar registros de PostgreSQL en Amazon Logs en la Guía del usuario de CloudWatch Amazon RDS](#).

[RDS.37] Los clústeres de bases de datos Aurora PostgreSQL deberían publicar registros en `Logs` `CloudWatch`

Requisitos relacionados: PCI DSS v4.0.1/10.4.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: `AWS::RDS::DBCluster`

Regla de AWS Config : [rds-aurora-postgresql-logs-to-cloudwatch](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de base de datos PostgreSQL de Amazon Aurora está configurado para publicar registros en `Amazon Logs`. `CloudWatch` El control falla si el clúster de base de datos Aurora PostgreSQL no está configurado para publicar registros de PostgreSQL en `Logs`. `CloudWatch`

El registro de base de datos proporciona detalles sobre las solicitudes realizadas a un clúster de RDS. Aurora PostgreSQL genera registros de eventos que contienen información útil para los administradores. La publicación de estos registros en `CloudWatch Logs` centraliza la administración

de registros y le ayuda a realizar análisis en tiempo real de los datos de registro. CloudWatch Logs retiene los registros en un almacenamiento muy duradero. También puede crear alarmas y ver las métricas en CloudWatch.

Corrección

Para publicar los registros del clúster de base de datos Aurora PostgreSQL en Logs, consulte CloudWatch Publicar registros de [Aurora PostgreSQL en Amazon Logs en la Guía del usuario de CloudWatch Amazon RDS](#).

[RDS.38] Las instancias de base de datos de RDS para PostgreSQL deben cifrarse en tránsito

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [rds-postgres-instance-encrypted-in-transit](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si una conexión a una instancia Amazon RDS for PostgreSQL de base de datos (DB) está cifrada en tránsito. El control falla si el `rds.force_ssl` parámetro del grupo de parámetros asociado a la instancia está establecido en `0` (desactivado). Este control no evalúa las instancias de base de datos de RDS que forman parte de un clúster de base de datos.

Los datos en tránsito hacen referencia a los datos que se mueven de una ubicación a otra, por ejemplo, entre los nodos del clúster o entre el clúster y la aplicación. Los datos pueden moverse a través de Internet o dentro de una red privada. El cifrado de los datos en tránsito reduce el riesgo de que un usuario no autorizado pueda espiar el tráfico de la red.

Corrección

Para exigir que todas las conexiones a su instancia de base de datos de RDS para PostgreSQL utilicen SSL, [consulte Uso de SSL con una instancia de base de datos de PostgreSQL](#) en la Guía del usuario de Amazon RDS.

[RDS.39] Las instancias de base de datos de RDS para MySQL deben cifrarse en tránsito

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [rds-mysql-instance-encrypted-in-transit](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si una conexión a una instancia Amazon RDS for MySQL de base de datos (DB) está cifrada en tránsito. El control falla si el `rds.require_secure_transport` parámetro del grupo de parámetros asociado a la instancia está establecido en `0` (desactivado). Este control no evalúa las instancias de base de datos de RDS que forman parte de un clúster de base de datos.

Los datos en tránsito hacen referencia a los datos que se mueven de una ubicación a otra, por ejemplo, entre los nodos del clúster o entre el clúster y la aplicación. Los datos pueden moverse a través de Internet o dentro de una red privada. El cifrado de los datos en tránsito reduce el riesgo de que un usuario no autorizado pueda espiar el tráfico de la red.

Corrección

Para exigir que todas las conexiones a su instancia de base de datos RDS para MySQL utilicen SSL, consulte la [compatibilidad con SSL/TLS para instancias de base de datos MySQL en Amazon RDS en la Guía del usuario de Amazon RDS](#).

[RDS.40] Las instancias de base de datos de RDS para SQL Server deberían publicar los registros en Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), (10), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 Nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.r5 SI-4 (20), Nist.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [rds-sql-server-logs-to-cloudwatch](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
logTypes	Lista de los tipos de registros que una instancia CloudWatch de base de datos de RDS para SQL Server debe configurarse para publicarlos en los registros. Este control produce un error si una instancia de base de datos no está configurada para publicar un tipo de registro especificado en la lista.	EnumList (máximo de 2 elementos)	agent, error	agent, error

Este control comprueba si una instancia de base de datos de Amazon RDS for Microsoft SQL Server está configurada para publicar registros en CloudWatch Amazon Logs. El control falla si la instancia de base de datos de RDS para SQL Server no está configurada para publicar registros en Logs. CloudWatch Si lo desea, puede especificar los tipos de registros que debe configurarse para publicar una instancia de base de datos.

El registro de la base de datos proporciona registros detallados de las solicitudes realizadas a una instancia de base de datos de Amazon RDS. La publicación de registros en CloudWatch Logs centraliza la administración de registros y le ayuda a realizar análisis de los datos de registro en

tiempo real. CloudWatch Logs conserva los registros en un almacenamiento muy duradero. Además, puede usarlo para crear alarmas para errores específicos que puedan producirse, como los reinicios frecuentes que se registran en un registro de errores. Del mismo modo, puede crear alarmas para los errores o advertencias que se registren en los registros de los agentes de SQL Server relacionados con las tareas de los agentes de SQL.

Corrección

Para obtener información sobre la publicación de registros en CloudWatch los registros de una instancia de base de datos de RDS para SQL Server, consulte los archivos de [registro de la base de datos de Amazon RDS para Microsoft SQL Server en la Guía del usuario de Amazon Relational Database Service](#).

[RDS.41] Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [rds-sqlserver-encrypted-in-transit](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si una conexión a una instancia de base de datos de Amazon RDS for Microsoft SQL Server está cifrada en tránsito. El control falla si el `rds.force_ssl` parámetro del grupo de parámetros asociado a la instancia de base de datos está establecido en. `0` (`off`)

Los datos en tránsito se refieren a los datos que se mueven de una ubicación a otra, por ejemplo, entre los nodos de un clúster de base de datos o entre un clúster de base de datos y una aplicación cliente. Los datos se pueden mover a través de Internet o dentro de una red privada. El cifrado de los datos en tránsito reduce el riesgo de que usuarios no autorizados escuchen el tráfico de la red.

Corrección

Para obtener información sobre cómo habilitar SSL/TLS las conexiones a instancias de base de datos de Amazon RDS que ejecutan Microsoft SQL Server, consulte [Uso de SSL con una instancia](#)

[de base de datos de Microsoft SQL Server](#) en la Guía del usuario de Amazon Relational Database Service.

[RDS.42] Las instancias de base de datos de RDS para MariaDB deberían publicar registros en Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), (9), NIST.800-53.r5 AC-6 (10) NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.r5 SI-4 (20), Nist.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [mariadb-publish-logs-to-cloudwatch-logs](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
logTypes	Una lista de los tipos de registros que una instancia de base de datos de MariaDB debe configurarse para publicar en Logs. CloudWatch El control genera una FAILED comprobación si una instancia de base de datos no está configurada para publicar un tipo de registro especificado en la lista.	EnumList (máximo de 4 elementos)	audit, error, general, slowquery	audit, error

Este control comprueba si una instancia de base de datos Amazon RDS for MariaDB está configurada para publicar determinados tipos de registros en Amazon Logs. CloudWatch El control falla si la instancia de base de datos MariaDB no está configurada para publicar los registros en Logs. CloudWatch Si lo desea, puede especificar qué tipos de registros debe configurarse para publicar una instancia de base de datos de MariaDB.

El registro de la base de datos proporciona registros detallados de las solicitudes realizadas a una instancia de base de datos Amazon RDS for MariaDB. La publicación de registros en Amazon CloudWatch Logs centraliza la administración de registros y le ayuda a realizar análisis en tiempo real de los datos de registro. Además, CloudWatch Logs conserva los registros en un almacenamiento duradero, lo que permite realizar revisiones y auditorías de seguridad, acceso y disponibilidad. Con CloudWatch Logs, también puede crear alarmas y revisar las métricas.

Corrección

Para obtener información sobre cómo configurar una instancia de base de datos Amazon RDS for MariaDB para publicar registros en Amazon Logs, [consulte Publicar registros de MariaDB en CloudWatch Amazon Logs en la Guía CloudWatch del usuario de Amazon Relational Database Service](#).

[RDS.44] El RDS para las instancias de base de datos MariaDB debe cifrarse en tránsito

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::RDS::DBInstance

Regla de AWS Config : [rds-mariadb-instance-encrypted-in-transit](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si las conexiones a una instancia de base de datos Amazon RDS for MariaDB están cifradas en tránsito. El control falla si el grupo de parámetros de base de datos asociado a la instancia de base de datos no está sincronizado o si el `require_secure_transport` parámetro del grupo de parámetros no está configurado en. ON

 Note

Este control no evalúa las instancias de base de datos de Amazon RDS que utilizan versiones de MariaDB anteriores a la 10.5. El `require_secure_transport` parámetro solo es compatible con las versiones 10.5 y posteriores de MariaDB.

Los datos en tránsito se refieren a los datos que se mueven de una ubicación a otra, por ejemplo, entre los nodos de un clúster de base de datos o entre un clúster de base de datos y una aplicación cliente. Los datos se pueden mover a través de Internet o dentro de una red privada. El cifrado de los datos en tránsito reduce el riesgo de que usuarios no autorizados escuchen el tráfico de la red.

Corrección

Para obtener información sobre cómo habilitar SSL/TLS las conexiones a una instancia de base de datos de Amazon RDS para MariaDB, [SSL/TLS consulte Obligaciones para todas las conexiones a una instancia de base de datos de MariaDB en la Guía del usuario de Amazon Relational Database Service](#).

Controles de Security Hub para Amazon Redshift

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon Redshift. Es posible que los controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Redshift.1] Los clústeres de Amazon Redshift deberían prohibir el acceso público

Requisitos relacionados: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (16) NIST.800-53.r5 AC-6, (20) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.4 2.1/1.3.6, PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: crítica

Tipo de recurso: AWS::Redshift::Cluster

Regla de AWS Config : [redshift-cluster-public-access-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los clústeres de Amazon Redshift son de acceso público. Evalúa el campo `PubliclyAccessible` del elemento de configuración del clúster.

El atributo de la configuración del clúster de Amazon Redshift `PubliclyAccessible` indica si el clúster es de acceso público. Si el clúster se configuró con `PubliclyAccessible` en `true`, se trata de una instancia orientada a Internet con un nombre DNS que se puede resolver públicamente y que se resuelve en una dirección IP pública.

Cuando el clúster no es accesible públicamente, se trata de una instancia interna con un nombre DNS que se resuelve en una dirección IP privada. A menos que desee que su clúster sea de acceso público, el clúster no debe configurarse con el valor `PubliclyAccessible` establecido como `true`.

Corrección

Para actualizar un clúster de Amazon Redshift para inhabilitar el acceso público, consulte [Modificación de un clúster](#) en la Guía de administración de Amazon Redshift. Establezca `Accesible públicamente` en `No`.

Las conexiones a los clústeres de Amazon Redshift [Redshift.2] deben cifrarse en tránsito

Requisitos relacionados: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 3 (NIST.800-53.r5 SC-23), NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0.1/4.2.1

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: `AWS::Redshift::Cluster` `AWS::Redshift::ClusterParameterGroup`

Regla de AWS Config : [redshift-require-tls-ssl](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las conexiones a los clústeres de Amazon Redshift son necesarias para utilizar el cifrado en tránsito. La comprobación no se realiza correctamente si el parámetro de clúster de Amazon Redshift `require_ssl` no se ha establecido como `True`.

El TLS se puede utilizar para evitar que posibles atacantes utilicen ataques similares para espiar person-in-the-middle o manipular el tráfico de la red. Solo se deben permitir las conexiones cifradas a través de TLS. El cifrado de los datos en tránsito puede afectar al rendimiento. Debe probar su aplicación con esta característica para comprender el perfil de rendimiento y el impacto del TLS.

Corrección

Para actualizar un grupo de parámetros de Amazon Redshift para que requiera el cifrado, consulte [Modificación de un grupo de parámetros](#) en la Guía de administración de Amazon Redshift.

Establecer `require_ssl` como `True`.

Los clústeres de Amazon Redshift [Redshift.3] deben tener habilitadas las instantáneas automáticas

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), (10), NIST.800-53.r5 SI-13 NIST.800-53.r5 SC-7 (5)

Categoría: Recuperación > Resiliencia > Respaldos habilitados

Gravedad: media

Tipo de recurso: `AWS::Redshift::Cluster`

Regla de AWS Config : [redshift-backup-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub	
MinRetentionPeriod	Periodo mínimo de retención de instantáneas en días	Entero	De 7 a 35	7	

Este control comprueba si un clúster de Amazon Redshift tiene habilitadas las instantáneas automatizadas y si el periodo de retención es superior o igual al periodo especificado. Se produce un error en el control si las instantáneas automatizadas no están habilitadas para el clúster o si el periodo de retención es inferior al periodo especificado. A menos que se proporcione un valor personalizado de parámetro para el periodo de retención de instantáneas, Security Hub utiliza un valor predeterminado de 7 días.

Las copias de seguridad le ayudan a recuperarse más rápidamente de un incidente de seguridad. Refuerzan la resiliencia de sus sistemas. Amazon Redshift toma instantáneas periódicas de forma predeterminada. Este control comprueba si las instantáneas automáticas están habilitadas y conservadas durante al menos siete días. Para obtener más información sobre las instantáneas automatizadas de Amazon Redshift, consulte [Instantáneas automatizadas](#) en la Guía de administración de Amazon Redshift.

Corrección

Para actualizar el período de retención de instantáneas de un clúster de Amazon Redshift, consulte [Modificación de un clúster](#) en la Guía de administración de Amazon Redshift. Para Copia de seguridad, establezca la Retención de instantáneas en un valor de 7 o superior.

Los clústeres de Amazon Redshift [Redshift.4] deben tener habilitado el registro de auditoría

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), (9), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.2.1

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::Redshift::Cluster

Regla de AWS Config : redshift-cluster-audit-logging-enabled (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

- loggingEnabled = true (no personalizable)

Este control comprueba si un clúster de Amazon Redshift tiene activado el registro de auditoría.

El registro de auditoría de Amazon Redshift proporciona información adicional acerca de las conexiones y las actividades de los usuarios en su clúster. Estos datos se pueden almacenar y proteger en Amazon S3 y pueden ser útiles en las auditorías e investigaciones de seguridad. Para obtener más información, consulte [Registro de auditoría de base de datos](#) en la Guía de administración de Amazon Redshift.

Corrección

Para configurar el registro de auditoría para un clúster de Amazon Redshift, consulte [Configuración de la auditoría mediante la consola](#) en la Guía de administración de Amazon Redshift.

Amazon Redshift [Redshift.6] debería tener habilitadas las actualizaciones automáticas a las versiones principales

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NiSt.800-53.r5 SI-2, NiSt.800-53.r5 SI-2 (2), NiSt.800-53.r5 SI-2 (4), NiSt.800-53.r5 SI-2 (5)

Categoría: Identificar > Administración de vulnerabilidades, parches y versiones

Gravedad: media

Tipo de recurso: AWS::Redshift::Cluster

Regla de AWS Config : [redshift-cluster-maintenancesettings-check](#)

Tipo de horario: provocado por un cambio

Parámetros:

- allowVersionUpgrade = true (no personalizable)

Este control comprueba si las actualizaciones automáticas de las versiones principales están habilitadas para el clúster de Amazon Redshift.

La activación de las actualizaciones automáticas de las versiones principales garantiza que las últimas actualizaciones de las versiones principales de los clústeres de Amazon Redshift se instalen durante el período de mantenimiento. Estas actualizaciones pueden incluir parches de seguridad y correcciones de errores. Mantenerse al día con la instalación de los parches es un paso importante para proteger los sistemas.

Corrección

Para solucionar este problema AWS CLI, utilice el comando Amazon `modify-cluster` Redshift y `--allow-version-upgrade` defina el atributo. *clustername* es el nombre de su clúster de Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

Los clústeres de Redshift [Redshift.7] deberían utilizar un enrutamiento de VPC mejorado

Requisitos relacionados: NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoría: Proteger > Configuración de red segura > Acceso privado a la API

Gravedad: media

Tipo de recurso: AWS::Redshift::Cluster

Regla de AWS Config : [redshift-enhanced-vpc-routing-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de Amazon Redshift ha habilitado EnhancedVpcRouting.

El Enhanced VPC Routing fuerza a todo COPY y el tráfico de UNLOAD entre el clúster y los repositorios de datos para que pase a través de su VPC. A continuación, puede utilizar las funciones de la VPC, como los grupos de seguridad y las listas de control de acceso a la red, para proteger el tráfico de la red. También puede usar Registros de flujo de VPC para monitorear el tráfico de red.

Corrección

Para obtener instrucciones de corrección detalladas, consulte [Habilitar el enrutamiento de VPC mejorado](#) en la Guía de administración de Amazon Redshift.

Los clústeres de Amazon Redshift [Redshift.8] no deben usar el nombre de usuario de administrador predeterminado

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Identificar > Configuración de recursos

Gravedad: media

Tipo de recurso: AWS::Redshift::Cluster

Regla de AWS Config : [redshift-default-admin-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de Amazon Redshift ha cambiado el nombre de usuario de administrador con respecto a su valor predeterminado. Este control fallará si el nombre de usuario de administrador de un clúster de Redshift se ha establecido como `awsuser`.

Al crear un clúster de Redshift, debe cambiar el nombre de usuario de administrador predeterminado por un valor único. Los nombres de usuario predeterminados son de dominio público y deben cambiarse al configurarlos. Cambiar los nombres de usuario predeterminados reduce el riesgo de accesos no deseados.

Corrección

No se puede cambiar el nombre de usuario de administración de su clúster de Amazon Redshift después de crearlo. Para crear un clúster nuevo con un nombre de usuario que no sea el predeterminado, consulte [Paso 1: crear un clúster de Amazon Redshift de muestra](#) en la Guía de introducción a Amazon Redshift.

Los clústeres de Redshift [Redshift.9] no deben usar el nombre de base de datos predeterminado

Requisitos relacionados: (1), NIST.800-53.r5 CM-2 NIST.800-53.r5 CA-9

Categoría: Identificar > Configuración de recursos

Gravedad: media

Tipo de recurso: AWS::Redshift::Cluster

Regla de AWS Config : [redshift-default-db-name-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un clúster de Amazon Redshift ha cambiado el nombre de la base de datos con respecto a su valor predeterminado. El control fallará si el nombre de la base de datos de un clúster de Redshift se ha establecido como dev.

Al crear un clúster de Redshift, debe cambiar el nombre predeterminado de la base de datos por un valor único. Los nombres predeterminados son de dominio público y deben cambiarse al configurarlos. Por ejemplo, un nombre conocido podría provocar un acceso inadvertido si se utilizara en las condiciones de la política de IAM.

Corrección

No se puede cambiar el nombre de la base de datos de su clúster de Amazon Redshift después de crearlo. Para obtener instrucciones sobre cómo crear un nuevo clúster, consulte [Introducción a Amazon Redshift](#) en la Guía de introducción a Amazon Redshift.

Los clústeres de Redshift [Redshift.10] deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 NIST.800-53.r5 SC-2 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::Redshift::Cluster

Regla de AWS Config : [redshift-cluster-kms-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los clústeres de Amazon Redshift están cifrados en reposo. El control falla si un clúster de Redshift no está cifrado en reposo o si la clave de cifrado es diferente de la clave proporcionada en el parámetro de la regla.

En Amazon Redshift, puede activar el cifrado de la base de datos de los clústeres para proteger los datos en reposo. Cuando activa el cifrado para un clúster, se cifran los bloques de datos y metadatos del sistema para el clúster y sus instantáneas. El cifrado de los datos en reposo es una práctica recomendada, ya que añade una capa de administración del acceso a los datos. El cifrado de los clústeres de Redshift en reposo reduce el riesgo de que un usuario no autorizado pueda acceder a los datos almacenados en el disco.

Corrección

Para modificar un clúster de Redshift para que utilice el cifrado de KMS, consulte [Cambiar el cifrado de clústeres](#) en la Guía de administración de Amazon Redshift.

[Redshift.11] Los clústeres de Redshift deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Redshift::Cluster

Regla de AWS Config : tagged-redshift-cluster (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un clúster de Amazon Redshift tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el clúster no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el clúster no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws :`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre

ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un clúster de Redshift, consulte [Etiquetado de recursos en Amazon Redshift](#) en la Guía de administración de Amazon Redshift.

[Redshift.12] Las suscripciones a notificaciones de eventos de Redshift deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Redshift::EventSubscription

Regla de AWS Config : tagged-redshift-eventsubscription (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si una instantánea del clúster de Amazon Redshift tiene etiquetas con las claves específicas definidas en el parámetro requiredTagKeys. El control lanza un error si la

instantánea del clúster no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la instantánea de clúster no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws :`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una suscripción a notificaciones de eventos de Redshift, consulte [Etiquetado de recursos en Amazon Redshift](#) en la Guía de administración de Amazon Redshift.

[Redshift.13] Las instantáneas del clúster de Redshift deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Redshift::ClusterSnapshot`

Regla de AWS Config : tagged-redshift-clustersnapshot (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si una instantánea del clúster de Amazon Redshift tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si la instantánea del clúster no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la instantánea de clúster no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws :`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a la instantánea del clúster de Redshift, consulte [Etiquetado de recursos en Amazon Redshift](#) en la Guía de administración de Amazon Redshift.

[Redshift.14] Los grupos de subredes del clúster de Redshift deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Redshift::ClusterSubnetGroup`

Regla de AWS Config : `tagged-redshift-cluster subnetgroup` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas	No default value

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.		que cumplan con AWS los requisitos .	

Este control comprueba si un grupo de subredes del clúster de Amazon Redshift tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza un error si el grupo de subredes del clúster no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el grupo de subredes del clúster no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un grupo de subredes del clúster de Redshift, consulte [Etiquetado de recursos en Amazon Redshift](#) en la Guía de administración de Amazon Redshift.

[Redshift.15] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos

Requisitos relacionados: PCI DSS v4.0.1/1.3.1

Categoría: Proteger > Configuración de red segura > Configuración de grupos de seguridad

Gravedad: alta

Tipo de recurso: `AWS::Redshift::Cluster`

Regla de AWS Config : [redshift-unrestricted-port-access](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un grupo de seguridad asociado a un clúster de Amazon Redshift ha establecido reglas de entrada que permiten acceder al puerto del clúster desde Internet (0.0.0.0/0 o ::/0). El control lanza un error si las reglas de entrada del grupo de seguridad permiten el acceso al puerto del clúster desde Internet.

Permitir el acceso al puerto del clúster de Redshift (dirección IP con el sufijo /0) sin restricciones puede provocar un acceso no autorizado o incidentes de seguridad. Recomendamos aplicar el principio de acceso con privilegio mínimo al crear grupos de seguridad y configurar las reglas de entrada.

Corrección

Para restringir la entrada en el puerto del clúster de Redshift a orígenes restringidos, consulte [Trabajar con reglas del grupo de seguridad](#) en la Guía del usuario de Amazon VPC. Actualice las reglas en las que el rango de puertos coincida con el puerto del clúster de Redshift y el rango de puertos IP sea 0.0.0.0/0.

[Redshift.16] Los grupos de subredes de clústeres de Redshift deben tener subredes de varias zonas de disponibilidad

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::Redshift::ClusterSubnetGroup

Regla de AWS Config : [redshift-cluster-subnet-group-multi-az](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

El control comprueba si un grupo de subredes de clústeres de Amazon Redshift tiene subredes de más de una zona de disponibilidad (AZ). El control falla si el grupo de subredes del clúster no tiene subredes de al menos dos subredes diferentes. AZs

La configuración de subredes en varias redes AZs ayuda a garantizar que su almacén de datos de Redshift pueda seguir funcionando incluso cuando se produzcan fallos.

Corrección

Para modificar un grupo de subredes de clústeres de Redshift para que abarque varios AZs, consulte [Modificación de un grupo de subredes de clústeres en la Guía de administración](#) de Amazon Redshift.

[Redshift.17] Los grupos de parámetros del clúster de Redshift deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Redshift::ClusterParameterGroup

Regla de AWS Config : [redshift-cluster-parameter-group-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Una lista de claves de etiquetas que no están en el sistema y que se deben asignar a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un grupo de parámetros de clúster de Amazon Redshift tiene las claves de etiqueta especificadas por el `requiredKeyTags` parámetro. El control produce un error si el grupo de parámetros no tiene ninguna clave de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no especifica ningún valor para el `requiredKeyTags` parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el grupo de parámetros no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws :` prefijo.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarle a identificar, organizar, buscar y filtrar los recursos. También pueden ayudarte a realizar un seguimiento de las acciones y notificaciones de los propietarios de los recursos. También puedes usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas](#).

 Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están pensadas para usarse con datos privados o confidenciales.

Corrección

Para obtener información sobre cómo añadir etiquetas a un grupo de parámetros de un clúster de Amazon Redshift, consulte [los recursos sobre etiquetas en Amazon Redshift en](#) la Guía de administración de Amazon Redshift.

Controles de Security Hub para Amazon Redshift Serverless

Estos AWS Security Hub controles de evalúan el servicio Amazon Redshift Serverless y sus recursos. Es posible que los controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado

Categoría: Proteger > Configuración de red segura > Recursos dentro de VPC

Gravedad: alta

Tipo de recurso: `AWS::RedshiftServerless::Workgroup`

Regla de AWS Config : [redshift-serverless-workgroup-routes-within-vpc](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el enrutamiento de VPC mejorado está habilitado para un grupo de trabajo de Amazon Redshift sin servidor. Se produce un error en el control si el enrutamiento de VPC mejorado está deshabilitado para el grupo de trabajo.

Si el enrutamiento de VPC mejorado está deshabilitado para un grupo de trabajo de Amazon Redshift Serverless, Amazon Redshift dirige el tráfico a través de Internet, incluido el tráfico a otros

servicios dentro de la red de. AWS Si habilita el enrutamiento de VPC mejorado para un grupo de trabajo, Amazon Redshift fuerza todo el UNLOAD tráfico entre el clúster COPY y los repositorios de datos a que pase por la nube virtual privada (VPC) en función del servicio Amazon VPC. Con el enrutamiento de VPC mejorado, puede usar las características de VPC estándar para controlar el flujo de los datos entre el clúster de Amazon Redshift y otros recursos. Esto incluye funciones como los grupos de seguridad de VPC y las políticas de puntos finales, las listas de control de acceso a la red (ACLs) y los servidores del sistema de nombres de dominio (DNS). También puede usar registros de flujo de la VPC para monitorear COPY y UNLOAD el tráfico.

Corrección

Para obtener más información sobre el enrutamiento de VPC mejorado y cómo habilitarlo para un grupo de trabajo, consulte [Control del tráfico de red con el enrutamiento de VPC mejorado de Redshift en](#) la Guía de administración de Amazon Redshift.

[RedshiftServerless.2] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::RedshiftServerless::Workgroup

Regla de AWS Config : [redshift-serverless-workgroup-encrypted-in-transit](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si las conexiones a un grupo de trabajo de Amazon Redshift Serverless son necesarias para cifrar los datos en tránsito. El control falla si el parámetro de `require_ssl` configuración del grupo de trabajo está establecido en. `false`

Un grupo de trabajo de Amazon Redshift Serverless es un conjunto de recursos informáticos que agrupa recursos informáticos como grupos de subredes de RPU VPC y grupos de seguridad. Las propiedades de un grupo de trabajo incluyen la configuración de redes y seguridad. Esta configuración específica si las conexiones a un grupo de trabajo deben utilizar SSL para cifrar los datos en tránsito.

Corrección

Para obtener información sobre cómo actualizar la configuración de un grupo de trabajo de Amazon Redshift Serverless para que requiera conexiones SSL, consulte Conexión a [Amazon Redshift Serverless en la Guía de administración de Amazon Redshift](#).

[RedshiftServerless.3] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: AWS::RedshiftServerless::Workgroup

Regla de AWS Config : [redshift-serverless-workgroup-no-public-access](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el acceso público está deshabilitado para un grupo de trabajo de Amazon Redshift sin servidor. Evalúa las `publiclyAccessible` propiedades de un grupo de trabajo de Redshift Serverless. Se produce un error en el control si el acceso público está habilitado (`true`) para el grupo de trabajo.

La configuración de acceso público (`publiclyAccessible`) de un grupo de trabajo de Amazon Redshift Serverless especifica si se puede acceder al grupo de trabajo desde una red pública. Si el acceso público está habilitado (`true`) para un grupo de trabajo, Amazon Redshift crea una dirección IP elástica que hace que el grupo de trabajo sea accesible públicamente desde fuera de la VPC. Si no quiere que un grupo de trabajo sea de acceso público, desactive su acceso público.

Corrección

Para obtener información sobre cómo cambiar la configuración de acceso público de un grupo de trabajo Amazon Redshift Serverless, consulte [Visualización de las propiedades de un grupo de trabajo en la Guía de administración de Amazon Redshift](#).

[RedshiftServerless.4] Los espacios de nombres de Redshift Serverless deben estar cifrados y gestionados por el cliente AWS KMS keys

Requisitos relacionados: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), (10), 2 NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-7 (NIST.800-53.r5 SC-12), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-2 NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::RedshiftServerless::Namespace

Regla de AWS Config : [redshift-serverless-namespace-cmk-encryption](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
kmsKeyArns	Una lista de nombres de recursos de Amazon (ARNs) AWS KMS keys para incluir en la evaluación. El control genera una FAILED búsqueda si un espacio de nombres de Redshift Serverless no está cifrado con	StringList (máximo de 3 elementos)	De 1 a 3 ARNs de las claves KMS existentes. Por ejemplo: arn:aws:kms:us-west-2:11112223333:key/1234abcd-12ab-34cd-56ef-1234567890ab .	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub

una clave KMS de la lista.

Este control comprueba si un espacio de nombres de Amazon Redshift sin servidor está cifrado en reposo con un servidor gestionado por el cliente. AWS KMS key El control falla si el espacio de nombres Redshift Serverless no está cifrado con una clave KMS administrada por el cliente. Si lo desea, puede especificar una lista de claves de KMS para que el control las incluya en la evaluación.

En Amazon Redshift sin servidor, un espacio de nombres define un contenedor lógico para objetos de base de datos. Este control comprueba periódicamente si la configuración de cifrado de un espacio de nombres especifica una clave de KMS administrada por el cliente AWS KMS key, en lugar de una AWS administrada, para el cifrado de los datos del espacio de nombres. Con una clave de KMS gestionada por el cliente, usted tiene el control total de la clave. Esto incluye definir y mantener la política de claves, administrar las concesiones, rotar el material criptográfico, asignar etiquetas, crear alias y habilitar y deshabilitar la clave.

Corrección

Para obtener información sobre cómo actualizar la configuración de cifrado de un espacio de nombres de Amazon Redshift Serverless y especificar un espacio de nombres gestionado por el cliente AWS KMS key, consulte [Cambiar el espacio de nombres de un espacio de nombres en la AWS KMS key Guía](#) de administración de Amazon Redshift.

Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado

Categoría: Identificar > Configuración de recursos

Gravedad: media

Tipo de recurso: AWS::RedshiftServerless::Namespace

Regla de AWS Config : [redshift-serverless-default-admin-check](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>validAdminUserNames</code>	Una lista de nombres de usuario de administrador que deben usar los espacios de nombres de Redshift Serverless. El control determina si un FAILED espacio de nombres utiliza un nombre de usuario de administrador que no está en la lista. La lista no puede especificar el valor predeterminado, <code>admin</code>	StringList (máximo de 6 elementos)	De 1 a 6 nombres de usuario de administrador válidos para los espacios de nombres de Redshift Serverless.	Sin valor predeterminado

Este control comprueba si el nombre de usuario de administrador de un espacio de nombres Amazon Redshift Serverless es el nombre de usuario de administrador predeterminado, `admin`. El control falla si el nombre de usuario de administrador del espacio de nombres Redshift Serverless es `admin`. Si lo desea, puede especificar una lista de nombres de usuario de administrador para que el control los incluya en la evaluación.

Al crear un espacio de nombres Amazon Redshift Serverless, debe especificar un nombre de usuario de administrador personalizado para el espacio de nombres. El nombre de usuario de administrador predeterminado es de conocimiento público. Al especificar un nombre de usuario de administrador personalizado, puedes, por ejemplo, ayudar a mitigar el riesgo o la eficacia de los ataques de fuerza bruta contra el espacio de nombres.

Corrección

Puede cambiar el nombre de usuario de administrador de un espacio de nombres de Amazon Redshift Serverless mediante la consola o la API de Amazon Redshift Serverless. Para cambiarlo mediante la consola, elija la configuración del espacio de nombres y, a continuación, elija Editar credenciales de administrador en el menú Acciones. [Para cambiarla mediante programación, utilice la UpdateNamespaceoperación o, si está utilizando la AWS CLI, ejecute el comando `update-namespace`](#). Si cambias el nombre de usuario de administrador, también debes cambiar la contraseña de administrador al mismo tiempo.

[RedshiftServerless.6] Los espacios de nombres de Redshift Serverless deberían exportar los registros a los registros CloudWatch

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::RedshiftServerless::Namespace

Regla de AWS Config : [redshift-serverless-publish-logs-to-cloudwatch](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un espacio de nombres de Amazon Redshift Serverless está configurado para exportar registros de conexión y usuario a Registros de Amazon Amazon Registros.

CloudWatch Se produce un error en el control si el espacio de nombres de Redshift sin servidor no está configurado para exportar los registros a Registros. CloudWatch

Si configura Amazon Redshift Serverless para que exporte los datos del registro de conexión (connectionlog) y del registro de usuario (userlog) a un grupo de CloudWatch registros de Amazon Logs, podrá recopilar y almacenar sus registros de registro en un almacenamiento duradero que permita realizar revisiones y auditorías de seguridad, acceso y disponibilidad. Con

CloudWatch Registros, también puede realizar análisis en tiempo real de los datos de registro y utilizar CloudWatch para crear alarmas y revisar métricas.

Corrección

Para exportar los datos de registro de un espacio de nombres de Amazon Redshift Serverless a Registros de CloudWatch Amazon Redshift Serverless, los registros respectivos se deben seleccionar para su exportación en los ajustes de configuración de registros de auditoría del espacio de nombres. Para obtener información sobre la actualización de estos ajustes, consulte [Edición de la seguridad y el cifrado](#) en la Guía de administración de Amazon Redshift.

Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de base de datos predeterminado

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Identificar > Configuración de recursos

Gravedad: media

Tipo de recurso: AWS::RedshiftServerless::Namespace

Regla de AWS Config : [redshift-serverless-default-db-name-check](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un espacio de nombres de Amazon Redshift Serverless utiliza el nombre de base de datos predeterminado,. dev El control falla si el espacio de nombres Redshift Serverless usa el nombre de base de datos predeterminado,. dev

Al crear un espacio de nombres Amazon Redshift Serverless, debe especificar un valor único y personalizado para el nombre de la base de datos y no utilizar el nombre de base de datos predeterminado, que es. dev El nombre de la base de datos predeterminado es Public Knoless. Al especificar un nombre de base de datos diferente, puede mitigar los riesgos, como el de que usuarios no autorizados accedan inadvertidamente a los datos del espacio de nombres.

Corrección

No se puede cambiar el nombre de la base de datos de un espacio de nombres de Amazon Redshift sin servidor después de crear el espacio de nombres. Sin embargo, puede especificar un nombre de

base de datos personalizado para un espacio de nombres Redshift Serverless al crear el espacio de nombres. Para obtener información sobre la creación de un espacio de nombres, consulte [Grupos de trabajo y espacios de nombres en la](#) Guía de administración de Amazon Redshift.

Controles de Security Hub para Route 53

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon Route 53.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Route53.1] Las comprobaciones de estado de Route 53 deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Route53::HealthCheck

AWS Config regla: tagged-route53-healthcheck (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control verifica si una comprobación de estado de Amazon Route 53 tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si la comprobación

de estado no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si la comprobación de estado no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, incluidas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una comprobación de estado de Route 53, consulte [Nombrar y etiquetar las comprobaciones de estado](#) en la Guía para desarrolladores de Amazon Route 53.

Las zonas alojadas públicas de Route 53 [Route53.2] deben registrar las consultas de DNS

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), (26), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 (9), Nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), Nist.800-53.r5 SI-4 (20), Nist.800-53.r5 SI-7 (8), PCI DSS v4.0.1/10.4.2 NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::Route53::HostedZone

Regla de AWS Config : [route53-query-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el registro de consultas de DNS está habilitado en una zona alojada pública de Amazon Route 53. El control falla si el registro de consultas de DNS no está habilitado en una zona alojada pública de Route 53.

Al registrar las consultas de DNS para una zona alojada de Route 53, se abordan los requisitos de seguridad y conformidad del DNS y se garantiza la visibilidad. Los registros incluyen información como el dominio o subdominio que se ha consultado, la fecha y la hora de la consulta, el tipo de registro de DNS (por ejemplo, A o AAAA) y el código de respuesta de DNS (por ejemplo, NoError o ServFail). Cuando el registro de consultas de DNS está habilitado, Route 53 publica los archivos de registro en Amazon CloudWatch Logs.

Corrección

Para registrar las consultas de DNS para las zonas alojadas públicas de Route 53, consulte [Configuración del registro de consultas de DNS](#) en la Guía para desarrolladores de Amazon Route 53.

Controles de Security Hub para Amazon S3

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon Simple Storage Service (Amazon S3). Es posible que los controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[S3.1] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.1.4, CIS AWS Foundations Benchmark v1.4.0/2.1.5, NIST.800-53.r5 AC-2 1,, NIST.800-53.r5 AC-3 (7), (21) NIST.800-53.r5

AC-3,, (11) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (16), (20) NIST.800-53.r5 AC-6, (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.1 1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: AWS:::Account

Regla de AWS Config : [s3-account-level-public-access-blocks-periodic](#)

Tipo de programa: Periódico

Parámetros:

- ignorePublicAcls: true (no personalizable)
- blockPublicPolicy: true (no personalizable)
- blockPublicAcls: true (no personalizable)
- restrictPublicBuckets: true (no personalizable)

Este control comprueba si la anterior configuración del bloqueo de acceso público de Amazon S3 está configurada en el nivel de cuenta para un bucket de uso general de S3. El control lanza un error si una o más de las configuraciones del bloqueo de acceso público se han establecido como false.

El control falla si alguna de las configuraciones se ha establecido como false o si alguna de las configuraciones no está configurada.

El bloque de acceso público de Amazon S3 está diseñado para proporcionar controles a nivel de bucket S3 completo Cuenta de AWS o individual a fin de garantizar que los objetos nunca tengan acceso público. El acceso público se concede a los depósitos y objetos mediante listas de control de acceso (ACLs), políticas de depósitos o ambas opciones.

A menos que quiera que se pueda acceder públicamente a sus buckets de S3, debe configurar la característica de Bloqueo de acceso público de Amazon S3 de nivel de cuenta.

Para obtener más información, consulte [Uso de Bloqueo de acceso público de Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.

Corrección

Para habilitar el acceso público por bloqueo de Amazon S3 para usted Cuenta de AWS, consulte [Configuración de los ajustes de bloqueo de acceso público para su cuenta](#) en la Guía del usuario de Amazon Simple Storage Service.

[S3.2] Los buckets de uso general de S3 deben bloquear el acceso público de lectura

Requisitos relacionados: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (11) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: AWS::S3::Bucket

Regla de AWS Config : [s3-bucket-public-read-prohibited](#)

Tipo de programa: periódico y activado por cambios

Parámetros: ninguno

Este control comprueba si un bucket de uso general de Amazon S3 permite el acceso público de lectura. Evalúa la configuración de Block Public Access, la política del bucket y la lista de control de acceso (ACL) del bucket. El control lanza un error si el bucket permite el acceso público de lectura.

Note

Si un bucket de S3 tiene una política de bucket, este control no evalúa las condiciones de la política que utilizan caracteres comodín o variables. Para obtener una PASSED conclusión, las condiciones de la política de bucket solo deben utilizar valores fijos, que son valores que no contienen caracteres comodín ni variables de política. Para obtener información sobre las variables de política, consulte [Variables y etiquetas](#) en la Guía del AWS Identity and Access Management usuario.

Algunos casos de uso probablemente requieran que todos en Internet puedan leer desde su bucket S3. Sin embargo, esas situaciones son poco habituales. Para garantizar la integridad y la seguridad de los datos, el bucket de S3 no debe tener acceso de lectura público.

Corrección

Para bloquear el acceso público de lectura en sus buckets de Amazon S3, consulte [Configuración de los ajustes de bloqueo de acceso público para sus buckets de S3](#) en la Guía del usuario de Amazon Simple Storage Service.

[S3.3] Los buckets de uso general de S3 deben bloquear el acceso público de escritura

Requisitos relacionados: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7), (21), (11), (16), (20) NIST.800-53.r5 AC-3, (21), (3) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (4) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: AWS : : S3 : : Bucket

Regla de AWS Config : [s3-bucket-public-write-prohibited](#)

Tipo de programa: periódico y activado por cambios

Parámetros: ninguno

Este control comprueba si un bucket de uso general de Amazon S3 permite el acceso público de escritura. Evalúa la configuración de Block Public Access, la política del bucket y la lista de control de acceso (ACL) del bucket. El control lanza un error si el bucket permite el acceso público de escritura.

Note

Si un bucket de S3 tiene una política de bucket, este control no evalúa las condiciones de la política que utilizan caracteres comodín o variables. Para obtener una PASSED conclusión, las condiciones de la política de bucket solo deben utilizar valores fijos, que son valores que

no contienen caracteres comodín ni variables de política. Para obtener información sobre las variables de política, consulte [Variables y etiquetas](#) en la Guía del AWS Identity and Access Management usuario.

Algunos casos de uso requieren que todos en Internet puedan escribir en su bucket S3. Sin embargo, esas situaciones son poco habituales. Para garantizar la integridad y la seguridad de los datos, el bucket de S3 no debe tener acceso de escritura público.

Corrección

Para bloquear el acceso público de escritura en sus buckets de Amazon S3, consulte [Configuración de los ajustes de bloqueo de acceso público para sus buckets de S3](#) en la Guía del usuario de Amazon Simple Storage Service.

[S3.5] En las solicitudes de los buckets de uso general de S3, se debe pedir el uso de SSL

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.1.1, CIS AWS Foundations Benchmark v1.4.0/2.1.2, NIST.800-53.r5 AC-1 7 (2), (1) NIST.800-53.r5 AC-4, 2 NIST.800-53.r5 IA-5 (3), 3, 3 (3), NIST.800-53.r5 SC-1 (4), NIST.800-53.r5 SC-2 (1), NIST.800-53.r5 SC-2 (NIST.800-53.r5 SC-12), NIST.800-53.r5 SC-7 Nist.800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), NIST.800-53.r5 SC-8 Nist.800-171.r2 3.13.8, NIST.800-171.r2 3.13.15, PCI DSS v3.2.1/4.1, PCI DSS v4.0.1/4.2.1 NIST.800-53.r5 SC-8

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS::S3::Bucket

Regla de AWS Config : [s3-bucket-ssl-requests-only](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un bucket de uso general de Amazon S3 tiene una política que exija que las solicitudes usen SSL. El control lanza un error si la política de buckets no requiere que las solicitudes exijan el uso de SSL.

Los buckets S3 deben tener políticas que exijan que todas las solicitudes (Action: S3:*) solo acepten la transmisión de datos a través de HTTPS en la política de recursos de S3, indicada mediante la clave de condición `aws:SecureTransport`.

Corrección

Para actualizar una política de bucket de Amazon S3 de manera que deniegue el transporte no seguro, consulte [Agregar una política de bucket mediante la consola de Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.

Añada una declaración de política similar a la de la siguiente política. Sustituya `amzn-s3-demo-bucket` por el nombre del bucket que está modificando.

```
{
  "Id": "ExamplePolicy",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSSLRequestsOnly",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "Bool": {
          "aws:SecureTransport": "false"
        }
      },
      "Principal": "*"
    }
  ]
}
```

Para obtener más información, consulta [¿Qué política de bucket de S3 debo usar para cumplir con la AWS Config regla s3-bucket-ssl-requests-only?](#) en el Centro de Conocimiento AWS Oficial.

[S3.6] Las políticas de compartimentos de uso general de S3 deberían restringir el acceso a otros Cuentas de AWS

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-171.r2 3.13.4

Categoría: Proteger > Gestión del acceso seguro > Se restringen las acciones de operaciones confidenciales de la API

Gravedad: alta

Tipo de recurso: AWS::S3::Bucket

Regla de AWS Config: [s3-bucket-blacklisted-actions-prohibited](#)

Tipo de horario: provocado por un cambio

Parámetros:

- `blacklistedactionpatterns`: `s3:DeleteBucketPolicy`, `s3:PutBucketAcl`, `s3:PutBucketPolicy`, `s3:PutEncryptionConfiguration`, `s3:PutObjectAcl` (no personalizable)

Este control comprueba si la política del bucket de uso general de Amazon S3 impide que las entidades principales de otras Cuentas de AWS realicen acciones denegadas en los recursos del bucket de S3. El control lanza un error si la política de buckets permite una o más de las acciones anteriores a una entidad principal en otra Cuenta de AWS.

La implementación del acceso con privilegios mínimos es esencial a la hora de reducir los riesgos de seguridad y el impacto de los errores o intentos malintencionados. Si una política de buckets S3 permite el acceso desde cuentas externas, podría provocar la exfiltración de datos por parte de una amenaza interna o de un atacante.

El parámetro `blacklistedactionpatterns` permite evaluar correctamente la regla para los buckets S3. El parámetro otorga acceso a cuentas externas para los patrones de acción que no están incluidos en la lista de `blacklistedactionpatterns`.

Corrección

Para actualizar una política de bucket de Amazon S3 para eliminar permisos, consulte [Agregar una política de bucket mediante la consola de Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.

En la página Editar política de bucket, en el cuadro de texto de edición de políticas, lleve a cabo una de las siguientes acciones:

- Elimine las declaraciones que otorgan a otras Cuentas de AWS el acceso a las acciones denegadas.
- Elimine las acciones denegadas permitidas de las declaraciones.

[S3.7] Los buckets de uso general de S3 deben usar la replicación entre regiones

Requisitos relacionados: PCI DSS v3.2.1/2.2, 6 (2), (2), NIST.800-53.r5 SI-13 (5) NIST.800-53.r5 AU-9(2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-3 NIST.800-53.r5 SC-5

Categoría: Proteger - Administración de acceso seguro

Gravedad: baja

Tipo de recurso: AWS : : S3 : : Bucket

AWS Config regla: [s3-bucket-cross-region-replication-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si los buckets de uso general de Amazon S3 tienen habilitada la replicación entre regiones. El control lanza un error si el bucket no tiene habilitada la replicación entre regiones.

La replicación es la copia automática y asíncrona de objetos entre depósitos iguales o diferentes. Regiones de AWS La replicación copia los objetos recientemente creados y las actualizaciones de objetos de un bucket de origen a un bucket o buckets de destino. Las mejores prácticas de AWS recomiendan la replicación de los buckets de origen y destino que son propiedad de la misma Cuenta de AWS. Además de la disponibilidad, debe plantearse otras configuraciones de protección de sistemas.

Este control produce un resultado FAILED para un bucket de destino de la replicación si no tiene habilitada la replicación entre regiones. Si hay una razón legítima por la que el bucket de destino no necesita que se habilite la replicación entre regiones, puede suprimir los resultados correspondientes a este bucket.

Corrección

Para habilitar la replicación entre regiones en un bucket S3, consulte [Configuración de la replicación para los buckets de origen y destino que pertenecen a la misma cuenta](#) en la Guía del usuario de

Amazon Simple Storage Service. En el Bucket de origen, seleccione Aplicar a todos los objetos del bucket.

[S3.8] Los buckets de uso general de S3 deben bloquear el acceso público

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.1.4, CIS AWS Foundations Benchmark v1.4.0/2.1.5 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-4 (7), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21),, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0.1/1.4.4

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Gravedad: alta

Tipo de recurso: AWS::S3::Bucket

Regla de AWS Config : [s3-bucket-level-public-access-prohibited](#)

Tipo de horario: provocado por un cambio

Parámetros:

- `excludedPublicBuckets` (no personalizable): una lista separada por comas de nombres de buckets de S3 públicos permitidos conocidos

Este control comprueba si un bucket de uso general de Amazon S3 bloquea el acceso público a nivel de bucket. El control lanza un error si alguna de las siguientes configuraciones se establece como false:

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`
- `restrictPublicBuckets`

Block Public Access a nivel de bucket de S3 proporciona controles para garantizar que los objetos nunca tengan acceso público. El acceso público se concede a los depósitos y objetos mediante listas de control de acceso (ACLs), políticas de depósitos o ambas.

A menos que quiera que se pueda acceder públicamente a sus buckets de S3, debe configurar la característica de Bloqueo de acceso público de Amazon S3 de nivel de bucket.

Corrección

Para obtener información sobre cómo eliminar el acceso público a nivel de bucket, consulte [Bloquear el acceso público a su almacenamiento de Amazon S3](#) en la Guía del usuario de Amazon S3.

[S3.9] Los buckets de uso general de S3 deben tener habilitado el registro de acceso al servidor

Requisitos relacionados: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), (9), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-3 (8), niST.800-53.r5 SI-4 (20), niST.800-53.r5 SI-7 (8), Nist.800-171.r2 3.3.8, PCI DSS v4.0.1/10.2.1

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS : : S3 : : Bucket

Regla de AWS Config : [s3-bucket-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el registro de acceso al servidor está habilitado para los buckets de uso general de Amazon S3. El control lanza un error si no está habilitado el registro de acceso al servidor. Cuando activa el registro, Amazon S3 envía los registros de acceso de un bucket de origen a un bucket de destino que usted selecciona. El bucket de destino debe estar en el Región de AWS mismo lugar que el bucket de origen y no debe tener configurado un período de retención predeterminado. El bucket de registro de destino no necesita tener activado el registro de acceso al servidor, por lo que debe suprimir los resultados de este bucket.

El registro de acceso al servidor brinda registros detallados de las solicitudes realizadas a un bucket. Los registros de acceso al servidor pueden ayudar en auditorías de acceso y seguridad. Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon S3: Habilitar el registro de acceso al servidor de Amazon S3](#).

Corrección

Para habilitar el registro de acceso al servidor Amazon S3, consulte [Habilitar el registro de acceso al servidor Amazon S3](#) en la Guía del usuario de Amazon S3.

[S3.10] Los buckets de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS : : S3 : : Bucket

Regla de AWS Config : [s3-version-lifecycle-policy-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un bucket de uso general de Amazon S3 con control de versiones tiene una configuración de ciclo de vida. El control lanza un error si el bucket no tiene una configuración de ciclo de vida.

Recomendamos configurar el ciclo de vida en el bucket de S3 para que pueda definir las acciones que desea que Amazon S3 realice durante la vida útil de un objeto.

Corrección

Para obtener más información sobre la configuración del ciclo de vida en un bucket de Amazon S3, consulte [Establecer la configuración del ciclo de vida en un bucket](#) y [Administrar el ciclo de vida de almacenamiento](#).

[S3.11] Los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos

Requisitos relacionados: NiSt.800-53.r5 SI-3 (8) NIST.800-53.r5 CA-7, NiSt.800-53.r5 SI-4, NiSt.800-53.r5 SI-4 (4), Nlst.800-171.r2 3.3.8

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::S3::Bucket

Regla de AWS Config : [s3-event-notifications-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
eventTypes	Lista de tipos de eventos de S3 preferidos	EnumList (máximo de 28 artículos)	s3: IntelligentTiering, s3:LifecycleExpiration:*, s3:LifecycleExpiration:Delete, s3:LifecycleExpiration:DeleteMarkerCreated, s3:LifecycleTransition, s3:ObjectAcl:Put, s3:ObjectCreated:*, ,	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
			s3:ObjectCreated:CompleteMultipartUpload, s3:ObjectCreated:Copy, s3:ObjectCreated:Post, s3:ObjectCreated:Put, s3:ObjectRemoved:* , s3:ObjectRemoved:Delete, s3:ObjectRemoved:DeleteMarkerCreated , s3:ObjectRestore:* , s3:ObjectRestore:Completed, s3:Object	

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
			Restore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:* , s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplication, s3:Replication:OperationMissedThreshold, s3:Replication:Op	

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
			rationNotTracked, s3:Replication:OperationReplicatedAfterThreshold, s3:TestEvent	

Este control comprueba si las notificaciones de eventos de S3 están habilitadas en un bucket de uso general de Amazon S3. El control lanza un error si las notificaciones de eventos de S3 no están habilitadas en el bucket. Si proporciona valores personalizados para el parámetro `eventTypes`, el control solo se aprueba si las notificaciones de eventos están habilitadas para los tipos de eventos especificados.

Al habilitar las notificaciones de eventos de S3, recibe alertas cuando se producen eventos específicos que afecten sus buckets de S3. Por ejemplo, puede recibir notificaciones sobre la creación, eliminación y restauración de objetos. Estas notificaciones pueden alertar a los equipos pertinentes sobre modificaciones accidentales o intencionales que puedan provocar el acceso no autorizado a los datos.

Corrección

Para obtener información sobre la detección de cambios en los buckets y objetos S3, consulte [Notificaciones de eventos de Amazon S3](#) en la Guía del usuario de Amazon S3.

[S3.12] no ACLs debe usarse para administrar el acceso de los usuarios a los depósitos de uso general de S3

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, (7), NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6

Categoría: Proteger - Administración de acceso seguro > Control de acceso

Gravedad: media

Tipo de recurso: AWS::S3::Bucket

Regla de AWS Config : [s3-bucket-acl-prohibited](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un bucket de uso general de Amazon S3 proporciona permisos de usuario con una lista de control de acceso (ACL). El control lanza un error si las ACL están configuradas para administrar el acceso de los usuarios a los buckets.

ACLs son mecanismos de control de acceso heredados anteriores a la IAM. En lugar de hacerlo ACLs, le recomendamos que utilice políticas de bucket de S3 o políticas AWS Identity and Access Management (IAM) para administrar el acceso a sus buckets de S3.

Corrección

Para superar este control, debes inhabilitarlo ACLs para tus buckets de S3. Para obtener instrucciones, consulta [Cómo controlar la propiedad de los objetos y deshabilitar ACLs tu depósito](#) en la Guía del usuario de Amazon Simple Storage Service.

Para crear una política de bucket S3, consulte [Agregar una política de bucket mediante la consola de Amazon S3](#). Para crear una política de usuario de IAM en un bucket de S3, consulte [Controlar el acceso a un bucket con políticas de usuario](#).

[S3.13] Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoría: Proteger > Protección de datos

Gravedad: baja

Tipo de recurso: AWS::S3::Bucket

Regla de AWS Config : [s3-lifecycle-policy-check](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
targetTransitionDays	Número de días después de crear los objetos cuando estos se trasladan a una clase de almacenamiento específico	Entero	De 1 a 36500	Sin valor predeterminado
targetExpirationDays	Número de días después de crear los objetos cuando estos se eliminan	Entero	De 1 a 36500	Sin valor predeterminado
targetTransitionStorageClasses	Tipo de clase de almacenamiento de S3 de destino	Enum	STANDARD_IA, INTELLIGENT_TIERING, ONEZONE_IA, GLACIER, GLACIER_IR, DEEP_ARCHIVE	Sin valor predeterminado

Este control comprueba si un bucket de uso general de Amazon S3 tiene una configuración de ciclo de vida. El control lanza un error si el bucket no tiene una configuración de ciclo de vida. Si proporciona valores personalizados para uno o varios de los parámetros anteriores, el control solo

pasa si la política incluye la clase de almacenamiento, el tiempo de eliminación o el tiempo de transición especificados.

Al generar una configuración de ciclo de vida para su bucket de S3, define las acciones que desea que Amazon S3 realice durante la vida útil de un objeto. Por ejemplo, puede realizar la transición de objetos a otra clase de almacenamiento, archivarlos o eliminarlos después de un periodo de tiempo especificado.

Corrección

Para obtener información sobre cómo configurar las políticas de ciclo de vida en un bucket de Amazon S3, consulte [Establecer la configuración del ciclo de vida en un bucket](#) y consulte [Administrar el ciclo de vida de almacenamiento](#) en la Guía del usuario de Amazon S3.

[S3.14] Los buckets de uso general de S3 deben tener habilitado el control de versiones

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Requisitos relacionados: NIST.800-53.r5 AU-9(2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6(1), NIST.800-53.r5 CP-6(2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5), NIST.800-171.r2 3.3.8

Gravedad: baja

Tipo de recurso: AWS::S3::Bucket

Regla de AWS Config : [s3-bucket-versioning-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un bucket de uso general de Amazon S3 tiene habilitado el control de versiones. El control lanza un error si se suspende el control de versiones del bucket.

El control de versiones conserva diversas variantes de un objeto en el mismo bucket de S3. Puede utilizar el control de versiones para conservar, recuperar y restaurar todas las versiones anteriores de los objetos almacenados en su bucket de S3. El control de versiones de S3 le ayuda a recuperarse de acciones no deseadas del usuario y de errores de la aplicación.

Tip

A medida que aumenta el número de objetos en un bucket debido al control de versiones, puede configurar el ciclo de vida para archivar o eliminar automáticamente los objetos con control de funciones en función de las reglas. Para obtener más información, consulte [Administración del ciclo de vida de los objetos versionados de Amazon S3](#).

Corrección

Para usar el control de versiones en un bucket de S3, consulte [Habilitar el control de versiones en buckets](#) en la Guía del usuario de Amazon S3.

[S3.15] Los buckets de uso general de S3 deben tener habilitado el bloqueo de objetos

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Requisitos relacionados: NIST.800-53.r5 CP-6 (2), PCI DSS v4.0.1/10.5.1

Gravedad: media

Tipo de recurso: AWS::S3::Bucket

AWS Config regla: [s3-bucket-default-lock-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
mode	Modo de retención de Bloqueo de objetos de S3	Enum	GOVERNANCE, COMPLIANCE	Sin valor predeterminado

Este control comprueba si un bucket de uso general de Amazon S3 tiene habilitado el bloqueo de objetos. El control lanza un error si el bloqueo de objetos no está habilitado para el bucket. Si proporciona un valor personalizado para el parámetro mode, el control solo pasa si el Bloqueo de objetos de S3 utiliza el modo de retención especificado.

Puede usar S3 Object Lock para almacenar objetos mediante un modelo write-once-read-many (WORM). S3 Bloqueo de objetos puede ayudar a evitar que se eliminen o se sobrescriban objetos durante un periodo de tiempo determinado o de manera indefinida. Puede usar Bloqueo de objetos de S3 para cumplir con los requisitos normativos que precisen de almacenamiento WORM o agregar una capa adicional de protección frente a cambios y eliminaciones de objetos.

Corrección

Para configurar Bloqueo de objetos para buckets de S3 nuevos y existentes, consulte [Configuración del Bloqueo de objetos de S3](#) en la Guía del usuario de Amazon S3.

[S3.17] Los depósitos de uso general de S3 deben cifrarse en reposo con AWS KMS keys

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Requisitos relacionados: NIST.800-53.r5 SC-1 2 (2), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, 8 (1), NIST.800-53.r5 SC-2 (10), (1), NIST.800-53.r5 SC-7 NiSt.800-53.r5 SI-7 NIST.800-53.r5 CA-9 (6), NiSt.800-53.r5 AU-9, NiSt.800-171.r2 3.8.9, NiSt.800-171.R2 3.13.16, PCI DSS v4.0.1/3.5.1

Gravedad: media

Tipo de recurso: AWS :: S3 :: Bucket

AWS Config Regla: [s3-default-encryption-kms](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un bucket de uso general de Amazon S3 está cifrado con un AWS KMS key (SSE-KMS o DSSE-KMS). El control lanza un error si el bucket se cifra con el cifrado predeterminado (SSE-S3).

El cifrado del servidor (SSE) es el cifrado de datos en su destino por la aplicación o servicio que los recibe. A menos que especifique lo contrario, los buckets S3 usan claves administradas de Amazon

S3 (SSE-S3) de forma predeterminada para el cifrado del servidor. Sin embargo, para mayor control, puede optar por configurar los buckets para que utilicen el cifrado del lado del servidor con AWS KMS keys (SSE-KMS o DSSE-KMS) en su lugar. Amazon S3 cifra los datos a nivel de objeto a medida que los escribe en los discos de los centros de AWS datos y los descifra automáticamente cuando accede a ellos.

Corrección

Para cifrar un bucket de S3 mediante SSE-KMS, consulte [Especificar el cifrado del lado del servidor con AWS KMS \(SSE-KMS\) en](#) la Guía del usuario de Amazon S3. Para cifrar un bucket de S3 mediante DSSE-KMS, consulte [Especificar el cifrado de doble capa del lado del servidor con AWS KMS keys \(DSSE-KMS\)](#) en la Guía del usuario de Amazon S3.

[S3.19] Los puntos de acceso de S3 deben tener habilitada la configuración de Bloqueo de acceso público

Requisitos relacionados: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (16) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS NIST.800-53.r5 SC-7 v4.0.1/1.4.4 NIST.800-53.r5 SC-7

Categoría: Proteger > Gestión del acceso seguro > Recurso no accesible públicamente

Gravedad: crítica

Tipo de recurso: AWS::S3::AccessPoint

AWS Config regla: [s3-access-point-public-access-blocks](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un punto de acceso de Amazon S3 tiene habilitada la configuración de Bloqueo de acceso público. Se produce un error en el control si la configuración de Bloqueo de acceso público no está habilitada para el punto de acceso.

La característica Bloqueo de acceso público de Amazon S3 ayuda a administrar el acceso a sus recursos de S3 en tres niveles: cuenta, bucket y punto de acceso. La configuración de cada nivel se puede configurar de forma independiente, lo que permite tener diferentes niveles de

restricciones de acceso público para los datos. La configuración del punto de acceso no puede anular individualmente la configuración más restrictiva en los niveles superiores (nivel de cuenta o bucket asignado al punto de acceso). Por el contrario, la configuración a nivel del punto de acceso es acumulativa, lo que significa que complementa la configuración de los demás niveles y funciona junto con esta. A menos que pretenda que un punto de acceso de S3 sea de acceso público, debe habilitar la configuración de Bloqueo de acceso público.

Corrección

Amazon S3 actualmente no admite cambiar la configuración de bloqueo de acceso público de un punto de acceso después de que se haya creado el punto de acceso. Todas las configuraciones de Bloqueo de acceso público están habilitadas de forma predeterminada al crear un punto de acceso nuevo. Le recomendamos que deje todas las configuraciones habilitadas a menos que sepa que tiene una necesidad específica de desactivar cualquiera de ellas. Para más información, consulte [Administración de acceso público a puntos de acceso](#) en la Guía del usuario de Amazon Simple Storage Service.

[S3.20] Los buckets de uso general de S3 deben tener habilitada la eliminación de MFA

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.1.2, CIS AWS Foundations Benchmark v1.4.0/2.1.3, (1), (2) NIST.800-53.r5 CA-9 NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5

Categoría: Proteger > Protección de datos > Protección contra la eliminación de datos

Gravedad: baja

Tipo de recurso: AWS::S3::Bucket

Regla de AWS Config : [s3-bucket-mfa-delete-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la eliminación con autenticación multifactor (MFA) está habilitada para un bucket de uso general de Amazon S3. El control falla si la eliminación de MFA no está habilitada para el bucket. El control no produce resultados para los depósitos que tienen una configuración de ciclo de vida.

Si habilita el control de versiones para un bucket de uso general de S3, si lo desea, puede añadir otra capa de seguridad configurando la eliminación de MFA para el bucket. Si lo hace, el propietario del bucket debe incluir dos formas de autenticación en cualquier solicitud para eliminar una versión de un objeto del bucket o cambiar el estado de control de versiones del bucket. La eliminación de MFA proporciona seguridad adicional si, por ejemplo, las credenciales de seguridad del propietario del bucket se ven comprometidas. La eliminación mediante MFA también puede ayudar a evitar la eliminación accidental de cubos, ya que exige que el usuario que inicie la acción de eliminación demuestre la posesión física de un dispositivo de MFA con un código de MFA, lo que añade una capa adicional de fricción y seguridad a la acción de eliminación.

 Note

Este control produce un PASSED resultado solo si la eliminación de MFA está habilitada para el depósito de uso general de S3. Para habilitar la eliminación de MFA en un bucket, el control de versiones también debe estar habilitado para el bucket. El control de versiones de un bucket es un método para almacenar múltiples variaciones de un objeto S3 en el mismo bucket. Además, solo el propietario del bucket que haya iniciado sesión como usuario root puede habilitar la eliminación de MFA y realizar acciones de eliminación en el bucket. No puede usar MFA delete con un bucket que tenga una configuración de ciclo de vida.

Corrección

Para obtener información sobre cómo habilitar el control de versiones y configurar la eliminación de MFA para un bucket de S3, [consulte Configuración de la eliminación de MFA](#) en la Guía del usuario de Amazon Simple Storage Service.

[S3.22] Los buckets de uso general de S3 deben registrar eventos de escritura a nivel de objeto

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/3.8, PCI DSS v4.0.1/10.2.1

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS :: : Account

AWS Config regla: [cloudtrail-all-write-s3-data-event-check](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si una Cuenta de AWS tiene al menos un rastro AWS CloudTrail multirregional que registre todos los eventos de escritura de datos de los buckets de Amazon S3. El control lanza un error si la cuenta no tiene un registro de seguimiento de varias regiones que registre los eventos de escritura de datos en los buckets de S3.

Las operaciones de S3 a nivel de objeto, como `GetObject`, `DeleteObject` y `PutObject`, se denominan eventos de datos. De forma predeterminada, CloudTrail no registra los eventos de datos, pero puede configurar rutas para registrar los eventos de datos de los buckets de S3. Al habilitar el registro a nivel de objeto para los eventos de escritura de datos, puede registrar cada vez que se accede a un objeto (archivo) en un bucket de S3. Habilitar el registro a nivel de objeto puede ayudarle a cumplir los requisitos de conformidad de datos, realizar análisis de seguridad exhaustivos, supervisar patrones específicos de comportamiento de los usuarios y tomar medidas respecto a la actividad de las API a nivel de objeto en sus buckets de S3 mediante Amazon Events. Cuenta de AWS CloudWatch Este control produce un resultado PASSED si configura un registro de seguimiento de varias regiones que registre eventos de datos de solo escritura o de todo tipo para todos los buckets de S3.

Corrección

Para habilitar el registro a nivel de objeto para los buckets de S3, consulte [Habilitar el registro de CloudTrail eventos para los buckets y objetos de S3 en la Guía del usuario](#) de Amazon Simple Storage Service.

[S3.23] Los buckets de uso general de S3 deben registrar eventos de lectura a nivel de objeto

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/3.9, PCI DSS v4.0.1/10.2.1

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS:::Account

AWS Config regla: [cloudtrail-all-read-s3-data-event-check](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si una Cuenta de AWS tiene al menos un rastro AWS CloudTrail multirregional que registre todos los eventos de datos de lectura de los buckets de Amazon S3. El control lanza un error si la cuenta no tiene un registro de seguimiento de varias regiones que registre los eventos de lectura de datos en los buckets de S3.

Las operaciones de S3 a nivel de objeto, como `GetObject`, `DeleteObject` y `PutObject`, se denominan eventos de datos. De forma predeterminada, CloudTrail no registra los eventos de datos, pero puede configurar rutas para registrar los eventos de datos de los buckets de S3. Al habilitar el registro a nivel de objeto para los eventos de lectura de datos, puede registrar cada vez que se accede a un objeto (archivo) en un bucket de S3. Habilitar el registro a nivel de objeto puede ayudarle a cumplir los requisitos de conformidad de datos, realizar análisis de seguridad exhaustivos, supervisar patrones específicos de comportamiento de los usuarios y tomar medidas respecto a la actividad de las API a nivel de objeto en sus buckets de S3 mediante Amazon Events. Cuenta de AWS CloudWatch Este control produce un resultado PASSED si configura un registro de seguimiento de varias regiones que registre eventos de datos de solo lectura o de todo tipo para todos los buckets de S3.

Corrección

Para habilitar el registro a nivel de objeto para los buckets de S3, consulte [Habilitar el registro de CloudTrail eventos para los buckets y objetos de S3 en la Guía del usuario](#) de Amazon Simple Storage Service.

[S3.24] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público

Requisitos relacionados: PCI DSS v4.0.1/1.4.4

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: `AWS::S3::MultiRegionAccessPoint`

Regla de AWS Config : `s3-mrap-public-access-blocked` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un punto de acceso de varias regiones de Amazon S3 tiene habilitado el bloqueo de acceso público. El control lanza un error si el punto de acceso de varias regiones no tiene habilitado el bloqueo de acceso público.

Los recursos de acceso público pueden provocar accesos no autorizados, filtraciones de datos o explotación de vulnerabilidades. Restringir el acceso mediante autenticación y autorización permite proteger la información confidencial y mantener la integridad de sus recursos.

Corrección

Todas las configuraciones de bloqueo de acceso público están habilitadas de forma predeterminada para los puntos de acceso de varias regiones de S3. Para obtener más información, consulte [Bloqueo del acceso público con puntos de acceso de varias regiones de Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service. No puede cambiar la configuración de Bloquear acceso público después de que se cree el punto de acceso de varias regiones.

Controles de Security Hub para SageMaker IA

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon SageMaker AI. Es posible que los controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet

Requisitos relacionados: NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-3, (21), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (11), (16) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (20), (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.2.1, NIST.800-53.r5 SC-7 PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.4 2.1/1.3.6, PCI DSS v4.0.1/1.4.4

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: AWS::SageMaker::NotebookInstance

Regla de AWS Config : [sagemaker-notebook-no-direct-internet-access](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el acceso directo a Internet está deshabilitado para una instancia de SageMaker AI notebook. El control falla si el campo `DirectInternetAccess` está habilitado para la instancia de cuaderno.

Si configuras tu instancia de SageMaker IA sin una VPC, el acceso directo a Internet está habilitado de forma predeterminada en tu instancia. Debe configurar la instancia con una VPC y cambiar la configuración predeterminada a Deshabilitar: acceso a Internet a través de una VPC. Para entrenar o alojar modelos desde un ordenador portátil, necesita acceso a Internet. Para habilitar el acceso a Internet, su VPC debe tener un punto de conexión de interfaz (AWS PrivateLink) o una puerta de enlace NAT y un grupo de seguridad que permita las conexiones salientes. Para obtener más información sobre cómo conectar una instancia de notebook a los recursos de una VPC, consulte [Conectar una instancia de notebook a los recursos de una VPC en](#) la Guía para desarrolladores de Amazon SageMaker AI. También debe asegurarse de que el acceso a su configuración de SageMaker IA esté limitado únicamente a los usuarios autorizados. Restrinja los permisos de IAM que permiten a los usuarios cambiar la configuración y los recursos de la SageMaker IA.

Corrección

Después de crear una instancia de cuaderno, no se puede cambiar la configuración de acceso a Internet. En su lugar, puede detener, eliminar y volver a crear la instancia con el acceso a Internet bloqueado. Para eliminar una instancia de bloc de notas que permite el acceso directo a Internet, consulte [Utilizar instancias de bloc de notas para crear modelos: limpiar](#) en la Guía para desarrolladores de Amazon SageMaker AI. Para recrear una instancia de cuaderno que deniegue el acceso a Internet, consulte [Crear una instancia de cuaderno](#). En Red, acceso directo a Internet, seleccione Deshabilitar: acceso a Internet a través de una VPC.

[SageMaker.2] las instancias de SageMaker notebook deben lanzarse en una VPC personalizada

Requisitos relacionados: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7 (11)

NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoría: Proteger > Configuración de red segura > Recursos dentro de VPC

Gravedad: alta

Tipo de recurso: AWS::SageMaker::NotebookInstance

Regla de AWS Config : [sagemaker-notebook-instance-inside-vpc](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una instancia de Amazon SageMaker AI Notebook se lanza dentro de una nube privada virtual (VPC) personalizada. Este control falla si una instancia de SageMaker AI Notebook no se lanza en una VPC personalizada o si se lanza en la VPC del servicio de SageMaker IA.

Las subredes son un rango de direcciones IP de una VPC. Recomendamos mantener sus recursos dentro de una VPC personalizada siempre que sea posible para garantizar una protección de red segura de su infraestructura. Una Amazon VPC es una red virtual dedicada a usted. Cuenta de AWS Con una Amazon VPC, puede controlar el acceso a la red y la conectividad a Internet de sus instancias de SageMaker AI Studio y notebook.

Corrección

No se puede cambiar la configuración de VPC después de crear una instancia de cuaderno. En su lugar, puede detener, eliminar y volver a crear la instancia. Para obtener instrucciones, consulte [Uso de instancias de bloc de notas para crear modelos: limpieza](#) en la Guía para desarrolladores de Amazon SageMaker AI.

[SageMaker.3] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2)

Categoría: Proteger > Gestión del acceso seguro > Restricciones de acceso para los usuarios raíz

Gravedad: alta

Tipo de recurso: AWS::SageMaker::NotebookInstance

Regla de AWS Config : [sagemaker-notebook-instance-root-access-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el acceso root está activado en una instancia de bloc de notas de Amazon SageMaker AI. El control falla si el acceso root está activado en una instancia de bloc de notas de SageMaker IA.

Siguiendo el principio de privilegios mínimos, se recomienda restringir el acceso raíz a los recursos de la instancia para evitar un exceso de permisos involuntario.

Corrección

Para restringir el acceso root a las instancias de bloc de notas de SageMaker IA, consulte [Controlar el acceso root a una instancia de bloc de notas de SageMaker IA](#) en la Guía para desarrolladores de Amazon SageMaker AI.

[SageMaker.4] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1

Requisitos relacionados: NIST.800-53.r5 SC-3 6 NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-5, 3 NIST.800-53.r5 SA-1

Categoría: Recuperación > Resiliencia > Alta disponibilidad

Gravedad: media

Tipo de recurso: AWS::SageMaker::EndpointConfig

Regla de AWS Config : [sagemaker-endpoint-config-prod-instance-count](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si las variantes de producción de un punto final de Amazon SageMaker AI tienen un recuento de instancias inicial superior a 1. El control falla si las variantes de producción del punto de conexión tienen solo 1 instancia inicial.

Las variantes de producción que se ejecutan con un recuento de instancias superior a 1 permiten gestionar la redundancia de instancias Multi-AZ mediante SageMaker IA. La implementación de recursos en varias zonas de disponibilidad es una práctica AWS recomendada para proporcionar una alta disponibilidad en su arquitectura. La alta disponibilidad lo ayuda a recuperarse de los incidentes de seguridad.

 Note

Este control se aplica solo a la configuración del punto de conexión basada en instancias.

Corrección

Para obtener más información sobre los parámetros de la configuración de puntos finales, consulte [Crear una configuración de punto final](#) en la Guía para desarrolladores de Amazon SageMaker AI.

[SageMaker.5] SageMaker los modelos deberían bloquear el tráfico entrante

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: media

Tipo de recurso: AWS::SageMaker::Model

Regla de AWS Config : [sagemaker-model-isolation-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un modelo alojado en Amazon SageMaker AI bloquea el tráfico de red entrante. El control falla si el `EnableNetworkIsolation` parámetro del modelo hospedado está establecido en `False`

SageMaker El entrenamiento de IA y los contenedores de inferencia implementados están habilitados para Internet de forma predeterminada. Si no quieres que la SageMaker IA proporcione acceso a una red externa a tus contenedores de formación o inferencia, puedes habilitar el

aislamiento de la red. Si habilitas el aislamiento de la red, los contenedores no podrán realizar llamadas de red salientes, ni siquiera a otras personas. Servicios de AWS Además, no hay AWS credenciales disponibles para el entorno de ejecución del contenedor. Habilitar el aislamiento de la red ayuda a evitar el acceso no deseado a sus recursos de SageMaker IA desde Internet.

Corrección

Para obtener más información sobre el aislamiento de redes para modelos de SageMaker IA, consulte [Ejecutar contenedores de entrenamiento e inferencia en modo sin Internet](#) en la Guía para desarrolladores de Amazon SageMaker AI. Puede habilitar el aislamiento de la red al crear su trabajo o modelo de formación estableciendo el valor del EnableNetworkIsolation parámetro en. True

[SageMaker.6] Las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::SageMaker::AppImageConfig

Regla de AWS Config : [sagemaker-app-image-config-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Una lista de claves de etiquetas que no están en el sistema y que se deben asignar a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si la configuración de imagen de una aplicación Amazon SageMaker AI (AppImageConfig) tiene las claves de etiqueta especificadas por el `requiredKeyTags` parámetro. El control falla si la configuración de la imagen de la aplicación no tiene ninguna clave de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no especificas ningún valor para el `requiredKeyTags` parámetro, el control solo comprueba la existencia de una clave de etiqueta y produce un error si la configuración de la imagen de la aplicación no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws :` prefijo.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarle a identificar, organizar, buscar y filtrar los recursos. También pueden ayudarte a realizar un seguimiento de las acciones y notificaciones de los propietarios de los recursos. También puedes usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas](#).

Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están pensadas para usarse con datos privados o confidenciales.

Corrección

Para añadir etiquetas a la configuración de imagen de una aplicación de Amazon SageMaker AI (AppImageConfig), puede utilizar la [AddTags](#) operación de la API de SageMaker IA o, si la utiliza AWS CLI, ejecutar el comando [add-tags](#).

[SageMaker.7] SageMaker las imágenes deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::SageMaker::Image

Regla de AWS Config : [sagemaker-image-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Una lista de claves de etiquetas no relacionadas con el sistema que se deben asignar a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una imagen de Amazon SageMaker AI tiene las claves de etiqueta especificadas por el `requiredKeyTags` parámetro. El control falla si la imagen no tiene ninguna clave de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no especifica ningún valor para el `requiredKeyTags` parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si la imagen no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws:` prefijo.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarle a identificar, organizar, buscar y filtrar los recursos. También pueden ayudarte a realizar un seguimiento de las acciones y notificaciones de los propietarios de los recursos. También puedes usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas](#).

 Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están pensadas para usarse con datos privados o confidenciales.

Corrección

Para añadir etiquetas a una imagen de Amazon SageMaker AI, puede utilizar la [AddTags](#) operación de la API de SageMaker IA o, si está utilizando la AWS CLI, ejecutar el comando [add-tags](#).

[SageMaker.8] las instancias de SageMaker notebook deberían ejecutarse en plataformas compatibles

Categoría: Detectar > Administración de vulnerabilidades, parches y versiones

Gravedad: media

Tipo de recurso: AWS::SageMaker::NotebookInstance

Regla de AWS Config : [sagemaker-notebook-instance-platform-version](#)

Tipo de programa: Periódico

Parámetros:

- supportedPlatformIdentifierVersions: notebook-a12-v1, notebook-a12-v2, notebook-a12-v3 (no personalizable)

Este control comprueba si una instancia de bloc de notas de Amazon SageMaker AI está configurada para ejecutarse en una plataforma compatible, en función del identificador de plataforma especificado para la instancia de portátil. El control falla si la instancia del bloc de notas está configurada para ejecutarse en una plataforma que ya no es compatible.

Si la plataforma de una instancia de bloc de notas de Amazon SageMaker AI ya no es compatible, es posible que no reciba parches de seguridad, correcciones de errores u otros tipos de actualizaciones. Es posible que las instancias de Notebook sigan funcionando, pero no recibirán actualizaciones de seguridad de SageMaker IA ni correcciones de errores críticos. Asumes los riesgos asociados

al uso de una plataforma no compatible. Para obtener más información, consulte el control de [JupyterLabversiones](#) en la Guía para desarrolladores de Amazon SageMaker AI.

Corrección

Para obtener información sobre las plataformas que Amazon SageMaker AI admite actualmente y cómo migrar a ellas, consulte las [instancias de notebook de Amazon Linux 2](#) en la Guía para desarrolladores de Amazon SageMaker AI.

Controles de Security Hub para Secrets Manager

Estos AWS Security Hub controles evalúan el AWS Secrets Manager servicio y los recursos.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[SecretsManager.1] Los secretos de Secrets Manager deberían tener habilitada la rotación automática

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0.1/8.6.3, PCI DSS v4.0.1/8.3.9

Categoría: Proteger - Desarrollo seguro

Gravedad: media

Tipo de recurso: AWS::SecretsManager::Secret

Regla de AWS Config : [secretsmanager-rotation-enabled-check](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
maximumAllowedRotation	Número máximo de días permitidos para la frecuencia de rotación del secreto	Entero	De 1 a 365	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub

tionFrequency

Este control comprueba si un secreto almacenado en él está configurado con rotación automática. AWS Secrets Manager Se produce un error en el control si el secreto no está configurado con rotación automática. Si proporciona un valor personalizado para el parámetro maximumAllowedRotationFrequency, el control solo pasa si el secreto gira automáticamente dentro del margen de tiempo especificado.

Secrets Manager le ayuda a mejorar la posición de seguridad de la organización. Los secretos incluyen credenciales de base de datos, contraseñas y claves de API de terceros. Puede usar Secrets Manager para almacenar secretos de forma centralizada, cifrarlos automáticamente, controlar el acceso a los secretos y renovar los secretos de forma segura y automática.

Secrets Manager puede renovar secretos. Puede usar la rotación para reemplazar los secretos a largo plazo por secretos a corto plazo. La renovar de sus secretos limita el tiempo que un usuario no autorizado puede usar un secreto comprometido. Por este motivo, debe renovar sus secretos con frecuencia. Para obtener más información sobre la rotación, [consulte Cómo girar AWS Secrets Manager los secretos](#) en la Guía del AWS Secrets Manager usuario.

Corrección

Para activar la rotación automática de los secretos de Secrets Manager, consulte [Configurar la rotación automática de AWS Secrets Manager los secretos mediante la consola](#) en la Guía del AWS Secrets Manager usuario. Debe elegir y configurar una AWS Lambda función de rotación.

[SecretsManager.2] Los secretos de Secrets Manager configurados con rotación automática deberían rotar correctamente

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0.1/8.6.3, PCI DSS v4.0.1/8.3.9

Categoría: Proteger - Desarrollo seguro

Gravedad: media

Tipo de recurso: `AWS::SecretsManager::Secret`

Regla de AWS Config : [secretsmanager-scheduled-rotation-success-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un secreto se ha rotado correctamente en función del programa de rotación. AWS Secrets Manager El control tiene errores si `RotationOccurringAsScheduled` es `false`. El control solo evalúa los secretos que tienen la renovación activada.

Secrets Manager le ayuda a mejorar la posición de seguridad de la organización. Los secretos incluyen credenciales de base de datos, contraseñas y claves de API de terceros. Puede usar Secrets Manager para almacenar secretos de forma centralizada, cifrarlos automáticamente, controlar el acceso a los secretos y renovar los secretos de forma segura y automática.

Secrets Manager puede renovar secretos. Puede usar la rotación para reemplazar los secretos a largo plazo por secretos a corto plazo. La renovación de sus secretos limita el tiempo que un usuario no autorizado puede usar un secreto comprometido. Por este motivo, debe renovar sus secretos con frecuencia.

Además de configurar los secretos para que giren automáticamente, debe asegurarse de que esos secretos giren correctamente según el programa de renovación.

Para obtener más información sobre la renovación, consulte [Cómo renovar sus secretos de AWS Secrets Manager](#) en la Guía del usuario de AWS Secrets Manager .

Corrección

Si se produce un error en la renovación automática, es posible que Secrets Manager haya detectado errores en la configuración. La rotación de secretos requiere el uso de una función de Lambda que defina cómo interactuar con la base de datos o el servicio al que pertenece el secreto.

Para obtener ayuda para diagnosticar y corregir errores comunes relacionados con la rotación de secretos, consulte [Solución de problemas de AWS Secrets Manager rotación de secretos](#) en la Guía del AWS Secrets Manager usuario.

[SecretsManager.3] Eliminar los secretos de Secrets Manager no utilizados

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15)

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS::SecretsManager::Secret

Regla de AWS Config : [secretsmanager-secret-unused](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
unusedForDays	Número máximo de días durante el que un secreto puede permanecer sin uso	Entero	De 1 a 365	90

Este control comprueba si se ha accedido a un AWS Secrets Manager secreto en el plazo especificado. Se produce un error en el control si un secreto no se utiliza más allá del periodo especificado. A menos que se proporcione un valor personalizado de parámetro para el periodo de acceso, Security Hub utiliza un valor predeterminado de 90 días.

Eliminar los secretos no utilizados es tan importante como renovarlos. Los antiguos usuarios pueden abusar de los secretos no utilizados, ya que ya no necesitan acceder a ellos. Además, a medida que más usuarios acceden a un secreto, es posible que alguien lo haya manipulado mal y lo haya filtrado a una entidad no autorizada, lo que aumenta el riesgo de abuso. Eliminar los secretos no utilizados ayuda a revocar el acceso secreto a los usuarios que ya no lo necesitan. También ayuda a reducir el costo de usar Secrets Manager. Por lo tanto, es esencial eliminar de forma rutinaria los secretos no utilizados.

Corrección

Para eliminar los secretos inactivos de Secrets Manager, consulte [Eliminar un AWS Secrets Manager secreto](#) en la Guía del AWS Secrets Manager usuario.

[SecretsManager.4] Los secretos de Secrets Manager deben rotarse en un número específico de días

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0.1/8.6.3, PCI DSS v4.0.1/8.3.9

Categoría: Proteger - Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS::SecretsManager::Secret

Regla de AWS Config : [secretsmanager-secret-periodic-rotation](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
maxDaysSinceRotation	Número máximo de días durante el que un secreto puede permanecer sin cambios	Entero	De 1 a 180	90

Este control comprueba si un secreto se rota al menos una vez dentro del período de tiempo especificado. AWS Secrets Manager Se produce un error en el control si no se rota un secreto al menos con esta frecuencia. A menos que se proporcione un valor personalizado de parámetro para el periodo de rotación, Security Hub utiliza un valor predeterminado de 90 días.

La rotación de los secretos puede ayudarle a reducir el riesgo de que se usen sus secretos sin autorización en su Cuenta de AWS. Los ejemplos incluyen credenciales de base de datos, contraseñas, claves de API de terceros e incluso texto arbitrario. Si no cambia sus secretos durante un largo período de tiempo, los secretos se vuelven más propensos a ser comprometidos.

Ya que hay más usuarios que acceden a un secreto, existen más probabilidades de que alguien haya cometido un error y lo haya filtrado a una entidad no autorizada. Los secretos se pueden

filtrar a través de registros y datos de caché. Pueden compartirse con fines de depuración y no pueden cambiarse ni revocarse una vez que se complete la depuración. Por todas estas razones, los secretos deben rotarse con frecuencia.

Puede configurar la renovación automática de los datos secretos en AWS Secrets Manager. Con la rotación automática, puede reemplazar secretos a largo plazo con secretos a corto plazo, lo cual reducirá significativamente el riesgo de peligro. Le sugerimos que configure la rotación automática para sus secretos de Secrets Manager. Para obtener más información, consulte [Rotación de sus secretos de AWS Secrets Manager](#) en la Guía del usuario de AWS Secrets Manager .

Corrección

Para activar la rotación automática de los secretos de Secrets Manager, consulte [Configurar la rotación automática de AWS Secrets Manager los secretos mediante la consola](#) en la Guía del AWS Secrets Manager usuario. Debe elegir y configurar una AWS Lambda función de rotación.

[SecretsManager.5] Los secretos de Secrets Manager deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::SecretsManager::Secret

Regla de AWS Config : tagged-secretsmanager-secret (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un AWS Secrets Manager secreto tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el secreto no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si el secreto no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un secreto de Secrets Manager, consulta [Etiquetar AWS Secrets Manager secretos](#) en la Guía del AWS Secrets Manager usuario.

Controles de Security Hub para Service Catalog

Estos AWS Security Hub controles evalúan el AWS Service Catalog servicio y los recursos.

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[ServiceCatalog.1] Las carteras de Service Catalog solo deben compartirse dentro de una AWS organización

Requisitos relacionados: NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-6
NIST.800-53.r5 CM-8, NIST.800-53.r5 SC-7

Categoría: Proteger - Administración de acceso seguro

Gravedad: alta

Tipo de recurso: AWS::ServiceCatalog::Portfolio

Regla de AWS Config : [service-catalog-shared-within-organization](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si AWS Service Catalog comparte carteras dentro de una organización cuando la integración con AWS Organizations está habilitada. El control falla si las carteras no se comparten dentro de una organización.

Compartir carteras solo dentro de Organizations permite garantizar que una cartera no se comparta con Cuentas de AWS incorrectas. Para compartir una cartera de Service Catalog con una cuenta de una organización, Security Hub recomienda utilizar ORGANIZATION_MEMBER_ACCOUNT en lugar de ACCOUNT. Esto simplifica la administración al regular el acceso otorgado a la cuenta en toda la organización. Si tiene una necesidad empresarial de compartir carteras de Service Catalog con una cuenta externa, puede [suprimir automáticamente los resultados](#) de este control o [deshabilitarlo](#).

Corrección

Para habilitar el uso compartido de carteras con Organizations, consulte [Compartir con AWS Organizations](#) en la Guía del administrador de Service Catalog.

Controles de Security Hub para Amazon SES

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon Simple Email Service (Amazon SES).

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[SES.1] Las listas de contactos de SES deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::SES::ContactList

Regla de AWS Config: tagged-ses-contactlist (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una lista de contactos de Amazon SES tiene etiquetas con claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si la lista de contactos no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si la lista de contactos no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los

propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a una lista de contactos de Amazon SES, consulte [TagResource](#) la referencia de la API v2 de Amazon SES.

[SES.2] Los conjuntos de configuración de SES deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::SES::ConfigurationSet

Regla de AWS Config: tagged-ses-configurationset (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un conjunto de configuración de Amazon SES tiene etiquetas con claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el conjunto de configuración no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el conjunto de configuración no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre

ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para añadir etiquetas a un conjunto de configuraciones de Amazon SES, consulte [TagResource](#) la referencia de la API v2 de Amazon SES.

Controles de Security Hub para Amazon SNS

Estos AWS Security Hub controles evalúan el servicio y los recursos del Amazon Simple Notification Service (Amazon SNS). Es posible que los controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[SNS.1] Los temas de SNS deben cifrarse en reposo mediante AWS KMS

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 (1), (10), NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (6), NIST.800-171.r2 3.13.11, NIST.800-171.r2 3.13.16 NIST.800-53.r5 SC-2

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::SNS::Topic

Regla de AWS Config : [sns-encrypted-kms](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un tema de Amazon SNS está cifrado en reposo utilizando claves administradas en AWS Key Management Service (AWS KMS). Los controles fallan si el tema de SNS no utiliza una clave de KMS para el cifrado del servidor (SSE). De forma predeterminada, SNS almacena los mensajes y archivos mediante el cifrado de disco. Para pasar este control, debe optar por utilizar una clave KMS para el cifrado. Esto agrega una capa adicional de seguridad y brinda una mayor flexibilidad de control de acceso.

El cifrado de los datos en reposo reduce el riesgo de que un usuario no autenticado acceda a los datos almacenados en el disco. AWS Se requieren permisos de API para descifrar los datos antes de

que puedan leerse. Recomendamos cifrar temas de SNS con claves de KMS para tener una capa de seguridad adicional.

Corrección

Para habilitar SSE para un tema de SNS, consulte [Habilitación del cifrado del servidor \(SSE\) para Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Antes de poder usar SSE, también debe configurar AWS KMS key políticas que permitan el cifrado de temas y el cifrado y descifrado de mensajes. Para obtener más información, consulte [Configuración de AWS KMS permisos](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

[SNS.2] Debe habilitarse el registro del estado de la entrega para los mensajes de notificación enviados a un tema

Important

Security Hub retiró este control en abril de 2024. Para obtener más información, consulte [Registro de cambios para los controles CSPM de Security Hub](#).

Requisitos relacionados: NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::SNS::Topic

Regla de AWS Config : [sns-topic-message-delivery-notification-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el registro está habilitado para el estado de entrega de los mensajes de notificación enviados a un tema de Amazon SNS para los puntos de conexión. Este control falla si la notificación del estado de entrega de los mensajes no está habilitada.

El registro es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de los servicios. El registro del estado de entrega de los mensajes aporta información operativa, como la siguiente:

- Saber si un mensaje se ha entregado al punto de enlace de Amazon SNS.
- Identificar la respuesta enviada desde el punto de enlace de Amazon SNS a Amazon SNS.
- Determinar el tiempo de permanencia del mensaje (el tiempo entre la marca de tiempo de publicación y la entrega a un punto de conexión de Amazon SNS).

Corrección

Para configurar el registro del estado de entrega de un tema, consulte el [Estado de entrega de los mensajes de Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

[SNS.3] Los temas de SNS deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::SNS::Topic`

Regla de AWS Config : `tagged-sns-topic` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un tema de Amazon SNS tiene etiquetas con claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si el tema no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza un error si el tema no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws :`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un tema de SNS, consulte [Configuración de etiquetas de temas de Amazon SNS](#) en la Guía para desarrolladores del servicio de Amazon Simple Notification Service.

[SNS.4] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: alta

Tipo de recurso: AWS::SNS::Topic

Regla de AWS Config : [sns-topic-no-public-access](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la política de acceso a los temas de Amazon SNS permite el acceso público. Este control falla si la política de acceso a los temas de Amazon SNS permite el acceso público.

Utiliza una política de acceso de Amazon SNS con un tema concreto para restringir quién puede trabajar con ese tema (por ejemplo, quién puede publicar mensajes en él o quién puede suscribirse a él). Las políticas de SNS pueden conceder acceso a otros Cuentas de AWS usuarios o a usuarios que estén dentro del suyo. Cuenta de AWS El uso de un carácter comodín (*) en el campo `Principal` de la política de temas y la falta de condiciones para limitar la política de temas pueden provocar la exfiltración de datos, la denegación del servicio o la inyección no deseada de mensajes en el servicio por parte de un atacante.

 Note

Este control no evalúa las condiciones de la política que utilizan caracteres comodín o variables. Para llegar a una PASSED conclusión, las condiciones de la política de acceso de Amazon SNS a un tema solo deben utilizar valores fijos, que son valores que no contienen caracteres comodín ni variables de política. Para obtener información sobre las variables de política, consulte [Variables y etiquetas](#) en la Guía del AWS Identity and Access Management usuario.

Corrección

Para actualizar las políticas de acceso de un tema de SNS, consulte [Información general sobre la administración del acceso en Amazon SNS](#) en la Guía para desarrolladores del servicio Amazon Simple Notification Service.

Controles de Security Hub para Amazon SQS

Estos AWS Security Hub controles evalúan el servicio y los recursos del Amazon Simple Queue Service (Amazon SQS). Es posible que los controles no estén disponibles en todos. Regiones de AWS Para obtener más información, consulte [Disponibilidad de los controles por región](#).

Las colas de Amazon SQS [SQS.1] deben cifrarse en reposo

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 8, NIST.800-53.r5 SC-2 8 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::SQS::Queue

Regla de AWS Config : sqs-queue-encrypted (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una cola de Amazon SQS está cifrada en reposo. El control falla si la cola no está cifrada con una clave administrada por SQL (SSE-SQS) o una AWS Key Management Service clave () (SSE-KMS).AWS KMS

El cifrado de los datos en reposo reduce el riesgo de que un usuario no autorizado acceda a los datos almacenados en el disco. El cifrado del lado del servidor (SSE) protege el contenido de los mensajes de las colas de SQS mediante claves de cifrado administradas por SQS (SSE-SQS) o claves (SSE-KMS). AWS KMS

Corrección

Para configurar el SSE para una cola de SQS, consulte [Configuración del cifrado del servidor \(SSE\) para una cola \(consola\)](#) en la Guía para desarrolladores de Amazon Simple Queue Service.

[SQS.2] Las colas de SQS deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS : :SQS : :Queue

Regla de AWS Config : tagged-sqs-queue (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredTagKeys	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si una cola de Amazon SQS tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla si la cola no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y falla si la cola no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para

sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una cola existente mediante la consola de Amazon SQS, consulte [Configuring cost allocation tags for an Amazon SQS queue \(console\)](#) en la Guía para desarrolladores de Amazon Simple Queue Service.

[SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público

Categoría: Proteger > Gestión del acceso seguro > Recurso no accesible públicamente

Gravedad: alta

Tipo de recurso: AWS::SQS::Queue

Regla de AWS Config : [sqs-queue-no-public-access](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una política de acceso de Amazon SQS permite el acceso público a una cola de SQS. El control falla si una política de acceso de SQS permite el acceso público a la cola.

Una política de acceso a Amazon SQS puede permitir el acceso público a una cola de SQS, lo que podría permitir que un usuario anónimo o cualquier identidad de AWS IAM autenticada accediera a la cola. Las políticas de acceso de SQS suelen proporcionar este acceso especificando el carácter

comodín (*) en el Principal elemento de la política, sin utilizar las condiciones adecuadas para restringir el acceso a la cola, o ambas cosas. Si una política de acceso de SQS permite el acceso público, es posible que terceros puedan realizar tareas como recibir mensajes de la cola, enviar mensajes a la cola o modificar la política de acceso de la cola. Esto podría provocar eventos como la exfiltración de datos, la denegación de servicio o la introducción de mensajes en la cola por parte de un agente de amenazas.

Note

Este control no evalúa las condiciones de la política que utilizan caracteres comodín o variables. Para obtener una PASSED conclusión, las condiciones de la política de acceso de Amazon SQS para una cola solo deben utilizar valores fijos, que son valores que no contienen caracteres comodín ni variables de política. Para obtener información sobre las variables de política, consulte [Variables y etiquetas](#) en la Guía del AWS Identity and Access Management usuario.

Corrección

Para obtener información sobre la configuración de la política de acceso de SQS para una cola de SQS, consulte [Uso de políticas personalizadas con el lenguaje de políticas de acceso de Amazon SQS en](#) la Guía para desarrolladores de Amazon Simple Queue Service.

Controles de Security Hub para Step Functions

Estos AWS Security Hub controles evalúan el AWS Step Functions servicio y los recursos.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[StepFunctions.1] Las máquinas de estado de Step Functions deberían tener el registro activado

Requisitos relacionados: PCI DSS v4.0.1/10.4.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::StepFunctions::StateMachine

Regla de AWS Config : [step-functions-state-machine-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
LogLevel	Nivel mínimo de registro	Enum	ALL, ERROR, FATAL	Sin valor predeterminado

Este control comprueba si una AWS Step Functions máquina de estado tiene activado el registro. El control falla si una máquina de estados no tiene el registro activado. Si proporciona un valor personalizado para el parámetro `LogLevel`, el control solo pasa si la máquina de estados tiene activado el nivel de registro especificado.

La monitorización le ayuda a mantener la fiabilidad, la disponibilidad y el rendimiento de Step Functions. Debe recopilar la mayor cantidad de datos de supervisión de los Servicios de AWS que utiliza para poder depurar más fácilmente los fallos multipunto. Tener una configuración de registro definida para sus máquinas de estado de Step Functions le permite realizar un seguimiento del historial de ejecución y los resultados en Amazon CloudWatch Logs. Si lo desea, puede realizar un seguimiento únicamente de los errores o eventos fatales.

Corrección

Para activar el registro en una máquina de estados de Step Functions, consulte [Configurar el registro](#) en la Guía para desarrolladores de AWS Step Functions .

[StepFunctions.2] Las actividades de Step Functions deben estar etiquetadas

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::StepFunctions::Activity`

AWS Config regla: `tagged-stepfunctions-activity` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si una AWS Step Functions actividad tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si la actividad no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si la actividad no está etiquetada con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan

operaciones cuando la etiqueta de la entidad principal coincide con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

 Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a una actividad de Step Functions, consulte [Etiquetado en Step Functions](#) en la Guía para desarrolladores de AWS Step Functions .

Controles de Security Hub para Systems Manager

Estos AWS Security Hub controles de evalúan el servicio y los recursos de AWS Systems Manager (SSM). Es posible que los controles de no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[SSM.1] EC2 Las instancias de Amazon deben administrarse mediante AWS Systems Manager

Requisitos relacionados: PCI DSS v3.2.1/2.4, NIST.800-53.r5 CA-9 (1), 5 (2), 5 (2), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8(1), NIST.800-53.r5 CM-8(2), NIST.800-53.r5 CM-8(3), NIST.800-53.r5 SA-1 5 (2), NIST.800-53.r5 SA-1 NIST.800-53.r5 SI-2 NIST.800-53.r5 SA-3

Categoría: Identificar - Inventario

Gravedad: media

Recurso evaluado: AWS::EC2::Instance

Recursos **AWS::EC2::Instance** de grabación AWS Config necesarios:
AWS::SSM::ManagedInstanceInventory

Regla de AWS Config : [ec2-instance-managed-by-systems-manager](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las EC2 instancias detenidas y en ejecución de su cuenta se administran mediante AWS Systems Manager. Systems Manager es un servicio de Servicio de AWS que puede utilizar para ver y controlar su AWS infraestructura en.

Para ayudarle a mantener la seguridad y la conformidad, Systems Manager analiza sus instancias administradas detenidas y en ejecución. Una instancia administrada es una máquina que está configurada para usarse con Systems Manager. Luego, Systems Manager informa o toma medidas correctivas sobre cualquier infracción de política que detecte. Systems Manager también lo ayuda a configurar y mantener sus instancias administradas.

Para obtener más información, consulte la [AWS Systems Manager Guía del usuario](#).

Corrección

Para gestionar EC2 instancias con Systems Manager, consulte [Amazon EC2 host Management](#) en la Guía del AWS Systems Manager usuario. En la sección Opciones de configuración, puede conservar las opciones predeterminadas o cambiarlas según sea necesario según la configuración que prefiera.

[SSM.2] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de parche de COMPLIANT después de la instalación de un parche

Requisitos relacionados: NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 SI-2 PCI DSS v3.2.1/6.2, PCI DSS v4.0.1/2.2.1, PCI DSS v4.0.1/6.3.3

Categoría: Detectar - Servicios de detección

Gravedad: alta

Tipo de recurso: AWS::SSM::PatchCompliance

Regla de AWS Config : [ec2-managedinstance-patch-compliance-status-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el estado de la conformidad de los parches de Systems Manager es COMPLIANT o NON_COMPLIANT después de instalar el parche en la instancia. El control falla si el estado de conformidad es NON_COMPLIANT. El control solo comprueba las instancias administradas por el Administrador de parches de Systems Manager.

Tener EC2 las instancias con parches según lo especificado por su organización reduce la superficie expuesta a ataques de su Cuentas de AWS.

Corrección

Systems Manager recomienda utilizar [políticas de parches](#) para configurar los parches para las instancias administradas. También puede utilizar los [documentos de Systems Manager](#), tal y como se describe en el siguiente procedimiento, para aplicar un parche a una instancia.

Para solucionar parches no conformes

1. Abra la AWS Systems Manager consola en. <https://console.aws.amazon.com/systems-manager/>
2. En Administración de nodos, elija Ejecutar comando y, a continuación, elija Ejecutar comando.
3. Seleccione la opción para AWS- RunPatchBaseline.
4. Cambie la Operation (Operación) a Install (Instalar).
5. Seleccione Elegir las instancias manualmente y, a continuación, elija las instancias no conformes.
6. Seleccione Ejecutar.
7. Una vez completado el comando, para monitorear el nuevo estado de conformidad de las instancias con parches, elija Conformidad en el panel de navegación.

[SSM.3] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8 (1), NIST.800-53.r5 SI-2 PCI DSS v4.0.1/2.2.1, PCI DSS v4.0.1/2.2.1, PCI DSS v4.0.1/2.2.1, PCI DSS v4.0.1/2.2.1

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::SSM::AssociationCompliance

Regla de AWS Config : [ec2-managedinstance-association-compliance-status-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el estado de conformidad de la AWS Systems Manager asociación es COMPLIANT o NON_COMPLIANT después de que la asociación se ejecute en una instancia. El control falla si el estado de conformidad de la asociación es NON_COMPLIANT.

Una asociación de State Manager es una configuración que se asigna a sus instancias administradas. La configuración define el estado que desea mantener en las instancias. Por ejemplo, una asociación puede especificar que el software antivirus debe estar instalado y ejecutándose en sus instancias, o bien que determinados puertos deben estar cerrados.

Después de crear una o varias asociaciones de administradores estatales, la información sobre el estado de la conformidad estará disponible inmediatamente. Puede ver el estado de conformidad en la consola o en respuesta a los AWS CLI comandos de o las acciones correspondientes de la API de Systems Manager. En el caso de las asociaciones, Conformidad de la configuración muestra el estado de conformidad (Compliant o Non-compliant). También muestra el nivel de gravedad asignado a la asociación, como Critical o Medium.

Para obtener más información sobre el cumplimiento de las asociaciones de gerentes estatales, consulte [Acerca del cumplimiento de las asociaciones de gerentes estatales](#) en la Guía del usuario de AWS Systems Manager .

Corrección

Una asociación fallida puede estar relacionada con diferentes factores, como los destinos y los nombres de los documentos de Systems Manager. Para solucionar este problema, primero debe identificar e investigar la asociación consultando el historial de asociaciones. Para obtener instrucciones sobre cómo ver el historial de asociaciones, consulte [Visualización del historial de asociaciones](#) en la Guía del usuario de AWS Systems Manager .

Tras investigar, puede editar la asociación para corregir el problema identificado. Puede editar una asociación para especificar un nuevo nombre, la programación, el nivel de gravedad o los destinos. Después de editar una asociación, AWS Systems Manager crea una nueva versión. Para obtener instrucciones sobre cómo editar una asociación, consulte [Edición y creación de una nueva versión de una asociación](#) en la Guía del usuario de AWS Systems Manager .

[SSM.4] Los documentos SSM no deben ser públicos

Requisitos relacionados: NIST.800-53.r5 AC-2 1 NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoría: Proteger > Configuración de red segura > Recursos no accesibles públicamente

Gravedad: crítica

Tipo de recurso: AWS::SSM::Document

Regla de AWS Config : [ssm-document-not-public](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si AWS Systems Manager los documentos de que son propiedad de la cuenta son públicos. Este control presenta errores si los documentos de Systems Manager que tienen el propietario Self son públicos.

Los documentos de Systems Manager que son públicos pueden permitir el acceso no deseado a sus documentos. Un documento público de Systems Manager puede exponer información valiosa sobre su cuenta, sus recursos y sus procesos internos.

A menos que su caso de uso requiera el uso compartido público, le recomendamos que bloquee la configuración de uso compartido público para los documentos de Systems Manager que son propiedad de Self.

Corrección

Para bloquear el uso compartido público de documentos de Systems Manager, consulte [Bloquear el uso compartido público de documentos de SSM](#) en la Guía del usuario de AWS Systems Manager .

[SSM.5] Los documentos SSM deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS : : SSM : : Document

Regla de AWS Config : [ssm-document-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Una lista de claves de etiquetas que no corresponden al sistema que se deben asignar a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un AWS Systems Manager documento tiene las claves de etiquetas especificadas en el `requiredKeyTags` parámetro. El control lanza error si el documento no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas por el `requiredKeyTags` parámetro. Si no especifica ningún valor para el `requiredKeyTags` parámetro, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el documento no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws :` prefijo. El control no evalúa los documentos de Systems Manager que son propiedad de Amazon.

Una etiqueta es una marca que se crea y asigna a un AWS recurso de. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. También pueden ayudarlo a realizar un seguimiento de las acciones y las notificaciones de los propietarios de los recursos. También puede utilizar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en](#)

[función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS recursos de etiquetado y la Guía del usuario de Tag Editor](#).

 Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Las etiquetas son accesibles desde muchos Servicios de AWS. No se han diseñado para usarse con información privada o confidencial.

Corrección

Para añadir etiquetas a un AWS Systems Manager documento, puede utilizar la [AddTagsToResource](#) operación de la AWS Systems Manager API o, si está utilizando la AWS CLI, ejecutar el [add-tags-to-resource](#) comando. También puede usar la consola de AWS Systems Manager .

Controles de Security Hub para AWS Transfer Family

Estos AWS Security Hub controles evalúan el AWS Transfer Family servicio y los recursos. Es posible que los controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

Los AWS Transfer Family flujos de trabajo de [Transfer.1] deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Transfer::Workflow`

Regla de AWS Config : `tagged-transfer-workflow` (regla personalizada de Security Hub)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredTagKeys</code>	Lista de claves de etiquetas que no corresponden al sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 artículos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	No default value

Este control comprueba si un AWS Transfer Family flujo de trabajo tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control lanza error si el flujo de trabajo no tiene ninguna clave de etiqueta o si no tiene todas las claves especificadas en el parámetro `requiredTagKeys`. Si no se proporciona el parámetro `requiredTagKeys`, el control solo comprueba la existencia de una clave de etiqueta y lanza error si el flujo de trabajo no está etiquetado con ninguna clave. Las etiquetas del sistema, que se aplican automáticamente y comienzan con `aws:`, se ignoran.

Una etiqueta es una etiqueta que se asigna a un AWS recurso y consta de una clave y un valor opcional. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Las etiquetas pueden ayudarlo a identificar, organizar, buscar y filtrar recursos. El etiquetado también ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Cuando utiliza el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, el cual define permisos en función de las etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a AWS los recursos. Puede crear una única política de ABAC o un conjunto independiente de políticas para sus entidades principales de IAM. Puede diseñar estas políticas de ABAC de manera que permitan operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿Para qué sirve ABAC? AWS](#) en la Guía del usuario de IAM.

Note

No agregue información de identificación personal (PII) ni otra información confidencial en las etiquetas. Muchas personas pueden acceder a las etiquetas Servicios de AWS, entre

ellas AWS Billing. Para obtener más información sobre las mejores prácticas de etiquetado, consulte [Etiquetar sus AWS recursos](#) en el. Referencia general de AWS

Corrección

Para agregar etiquetas a un flujo de trabajo de Transfer Family (consola)

1. Abre la consola. AWS Transfer Family
2. En el panel de navegación, elija Workflows (Flujos de trabajo). Luego, seleccione el flujo de trabajo que desea etiquetar.
3. Elija Administrar etiquetas y, a continuación, añada las etiquetas.

[Transfer.2] Los servidores de Transfer Family no deben utilizar el protocolo FTP para la conexión del punto de conexión

Requisitos relacionados: PCI NIST.800-53.r5 CM-7, NIST.800-53.r5 IA-5 DSS NIST.800-53.r5 SC-8 v4.0.1/4.2.1

Categoría: Proteger > Protección de datos > Cifrado de data-in-transit

Gravedad: media

Tipo de recurso: AWS::Transfer::Server

Regla de AWS Config : [transfer-family-server-no-ftp](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un AWS Transfer Family servidor utiliza un protocolo distinto del FTP para la conexión del punto final. El control lanza error si el servidor utiliza el protocolo FTP para que un cliente se conecte al punto de conexión del servidor.

El protocolo de transferencia de archivos (FTP) establece la conexión del punto de conexión mediante canales no cifrados, lo que hace que los datos enviados a través de estos canales sean vulnerables a la interceptación. El uso de SFTP (protocolo de transferencia de archivos SSH), FTPS (protocolo de transferencia de archivos seguro) o AS2 (declaración de aplicabilidad 2) ofrece un

nivel adicional de seguridad al cifrar los datos en tránsito y se puede utilizar para evitar que posibles atacantes utilicen ataques similares para espiar person-in-the-middle o manipular el tráfico de la red.

Corrección

Para modificar el protocolo de un servidor de Transfer Family, consulte [Edición de los protocolos de transferencia de archivos](#) en la Guía del usuario de AWS Transfer Family .

[Transfer.3] Los conectores Transfer Family deben tener habilitado el registro

Requisitos relacionados: NIST.800-53.r5 AC-2 (12), (4), NIST.800-53.r5 AC-2 (26), (9), NIST.800-53.r5 AC-4 (9), NIST.800-53.r5 AC-6 Nist.800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, Nist.800-53.r5 SI-4, Nist.800-53.r5 SI-4 (20), Nist.800-53.r5 SI-7 (8)

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::Transfer::Connector

Regla de AWS Config : [transfer-connector-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el CloudWatch registro de Amazon está habilitado para un AWS Transfer Family conector. El control falla si el CloudWatch registro no está activado en el conector.

Amazon CloudWatch es un servicio de supervisión y observabilidad que proporciona visibilidad de sus AWS recursos, incluidos los AWS Transfer Family recursos. Para Transfer Family, CloudWatch proporciona auditoría y registro consolidados del progreso y los resultados del flujo de trabajo. Esto incluye varias métricas que Transfer Family define para los flujos de trabajo. Puede configurar Transfer Family para que registre automáticamente los eventos del conector CloudWatch. Para ello, especifique una función de registro para el conector. Para la función de registro, debe crear una función de IAM y una política de IAM basada en los recursos que defina los permisos de la función.

Corrección

Para obtener información sobre cómo habilitar el CloudWatch registro para un conector Transfer Family, consulte [Amazon CloudWatch logging for AWS Transfer Family servers](#) en la Guía del AWS Transfer Family usuario.

[Transfer.4] Los acuerdos Transfer Family deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Transfer::Agreement

Regla de AWS Config : [transfer-agreement-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Una lista de claves de etiquetas que no están en el sistema y que se deben asignar a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un AWS Transfer Family acuerdo tiene las claves de etiqueta especificadas en el `requiredKeyTags` parámetro. El control produce un error si el acuerdo no tiene ninguna clave de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no especifica ningún valor para el `requiredKeyTags` parámetro, el control comprobará únicamente la existencia de una clave de etiqueta y fallará si el acuerdo no

tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws:` prefijo.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarle a identificar, organizar, buscar y filtrar los recursos. También pueden ayudarte a realizar un seguimiento de las acciones y notificaciones de los propietarios de los recursos. También puedes usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas](#).

 Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están pensadas para usarse con datos privados o confidenciales.

Corrección

Para obtener información sobre cómo añadir etiquetas a un AWS Transfer Family acuerdo, consulte los [métodos de etiquetado de recursos](#) en la Guía del usuario de Tagging AWS Resources y Tag Editor.

[Transfer.5] Los certificados de Transfer Family deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Transfer::Certificate`

Regla de AWS Config : [transfer-certificate-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Una lista de claves de etiquetas que no están en el sistema y que se deben asignar a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un AWS Transfer Family certificado tiene las claves de etiqueta especificadas en el `requiredKeyTags` parámetro. El control produce un error si el certificado no tiene ninguna clave de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no se especifica ningún valor para el `requiredKeyTags` parámetro, el control solo comprueba la existencia de una clave de etiqueta y produce un error si el certificado no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws:` prefijo.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarle a identificar, organizar, buscar y filtrar los recursos. También pueden ayudarte a realizar un seguimiento de las acciones y notificaciones de los propietarios de los recursos. También puedes usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas](#).

 **Note**

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están pensadas para usarse con datos privados o confidenciales.

Corrección

Para obtener información sobre cómo añadir etiquetas a un AWS Transfer Family certificado, consulte los [métodos de etiquetado de recursos](#) en la Guía del usuario sobre cómo etiquetar AWS los recursos y el editor de etiquetas.

[Transfer.6] Los conectores Transfer Family deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::Transfer::Connector

Regla de AWS Config : [transfer-connector-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
requiredKeyTags	Una lista de claves de etiquetas que no están en el sistema y que se deben asignar a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un AWS Transfer Family conector tiene las claves de etiqueta especificadas en el `requiredKeyTags` parámetro. El control falla si el conector no tiene ninguna clave de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no especifica ningún valor para el `requiredKeyTags` parámetro, el control solo comprueba la existencia de una clave de etiqueta y falla si el conector no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws:` prefijo.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarle a identificar, organizar, buscar y filtrar los recursos. También pueden ayudarte a realizar un seguimiento de las acciones y notificaciones de los propietarios de los recursos. También puedes usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas](#).

 Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están pensadas para usarse con datos privados o confidenciales.

Corrección

Para obtener información sobre cómo añadir etiquetas a un AWS Transfer Family conector, consulte los [métodos de etiquetado de recursos](#) en la Guía del usuario de Tagging AWS Resources y Tag Editor.

[Transfer.7] Los perfiles de Transfer Family deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::Transfer::Profile`

Regla de AWS Config : [transfer-profile-tagged](#)

Tipo de horario: provocado por un cambio

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
<code>requiredKeyTags</code>	Una lista de claves de etiquetas que no están en el sistema y que se deben asignar a un recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList (máximo de 6 elementos)	De 1 a 6 claves de etiquetas que cumplan con AWS los requisitos .	Sin valor predeterminado

Este control comprueba si un AWS Transfer Family perfil tiene las claves de etiqueta especificadas en el `requiredKeyTags` parámetro. El control falla si el perfil no tiene ninguna clave de etiqueta o no tiene todas las claves especificadas en el `requiredKeyTags` parámetro. Si no especifica ningún valor para el `requiredKeyTags` parámetro, el control solo comprobará la existencia de una clave de etiqueta y fallará si el perfil no tiene ninguna clave de etiqueta. El control ignora las etiquetas del sistema, que se aplican automáticamente y tienen el `aws :` prefijo. El control evalúa los perfiles locales y los perfiles de los socios.

Una etiqueta es una etiqueta que se crea y se asigna a un AWS recurso. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Utilice etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Pueden ayudarle a identificar, organizar, buscar y filtrar los recursos. También pueden ayudarte a realizar un seguimiento de las acciones y notificaciones de los propietarios de los recursos. También puedes usar etiquetas para implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización. Para obtener más información sobre las estrategias de ABAC, consulte [Definir permisos en función de los atributos con la autorización ABAC en](#) la Guía del usuario de IAM. Para obtener más información sobre las etiquetas, consulte los [AWS recursos de etiquetado y la Guía del usuario del editor de etiquetas](#).

 Note

No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS sitios. No están pensadas para usarse con datos privados o confidenciales.

Corrección

Para obtener información sobre cómo añadir etiquetas a un AWS Transfer Family perfil, consulte los [métodos de etiquetado de recursos](#) en la Guía del usuario sobre cómo etiquetar AWS los recursos y el editor de etiquetas.

Controles de Security para AWS WAF

Estos AWS Security Hub controles evalúan el AWS WAF servicio y los recursos. Es posible que los controles de no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

El registro AWS WAF Classic Global Web ACL de [WAF.1] debe estar habilitado

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (8), PCI DSS v4.0.1/10.4.2

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::WAF::WebACL

Regla de AWS Config : [waf-classic-logging-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el registro está habilitado para una ACL web de AWS WAF global. Este control falla si el registro no está habilitado para la ACL web.

El registro es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de los servicios de AWS WAF a nivel global. Es un requisito empresarial y de

conformidad en muchas organizaciones, y permite solucionar problemas de comportamiento de las aplicaciones. También proporciona información detallada sobre el tráfico que analiza la ACL web a la que se conecta AWS WAF.

Corrección

Para obtener más información acerca del registro de ACL AWS WAF web, consulte [Logging web ACL traffic information \(registro de información del tráfico de la ACL web\)](#) en la Guía para AWS WAF desarrolladores de.

Las reglas de [WAF.2] Regionales AWS WAF clásicas deben tener al menos una condición

Requisitos relacionados: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: AWS::WAFRegional::Rule

Regla de AWS Config : [waf-regional-rule-not-empty](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una regla de AWS WAF Regional tiene al menos una condición. El control falla si no hay condiciones presentes en una regla.

Una regla de WAF Regional puede contener varias condiciones. Las condiciones de la regla permiten inspeccionar el tráfico y realizar una acción definida (permitir, bloquear o contar). Sin ninguna condición, el tráfico pasa sin inspección. Una regla de WAF Regional sin condiciones, pero con un nombre o etiqueta que sugiera permitir, bloquear o contar, podría llevar a suponer erróneamente que se está produciendo una de esas acciones.

Corrección

Para añadir una condición a una regla vacía, consulta [Añadir y eliminar condiciones en una regla](#) en la Guía para desarrolladores de AWS WAF .

Los grupos de reglas de [WAF.3] Regionales AWS WAF clásicos deben tener al menos una regla

Requisitos relacionados: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: AWS::WAFRegional::RuleGroup

Regla de AWS Config : [waf-regional-rulegroup-not-empty](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de reglas de AWS WAF Regionales tiene al menos una regla. El control falla si no hay reglas presentes en un grupo de reglas.

Un grupo de reglas de WAF Regionales puede contener varias reglas. Las condiciones de la regla permiten inspeccionar el tráfico y realizar una acción definida (permitir, bloquear o contar). Sin ninguna regla, el tráfico pasa sin inspección. Un grupo de reglas de WAF Regionales sin reglas, pero con un nombre o etiqueta que sugiera permitir, bloquear o contar, podría llevar a suponer erróneamente que se está produciendo una de esas acciones.

Corrección

Para añadir reglas y condiciones de reglas a un grupo de reglas vacío, consulte [Añadir y eliminar reglas de un grupo de reglas de AWS WAF clásico](#) y [Añadir y eliminar condiciones en una regla](#) en la Guía para AWS WAF desarrolladores de.

La web de [WAF.4] Regionales AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: AWS::WAFRegional::WebACL

Regla de AWS Config : [waf-regional-webacl-not-empty](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una ACL AWS WAF Classic Regional web de contiene reglas de WAF o grupos de reglas de WAF. Este control falla si una ACL web no contiene ninguna regla o grupo de reglas de WAF.

Una ACL web de WAF Regional puede contener una colección de reglas y grupos de reglas que inspeccionan y controlan las solicitudes web. Si una ACL web está vacía, el tráfico web puede pasar sin que el WAF lo detecte ni actúe en consecuencia, según la acción predeterminada.

Corrección

Para añadir reglas o grupos de reglas a una ACL web de Regional AWS WAF clásica vacía, consulte [Edición de una ACL web](#) en la Guía para AWS WAF desarrolladores de.

Las reglas globales de [WAF.6] AWS WAF clásicas deben tener al menos una condición

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: AWS::WAF::Rule

Regla de AWS Config : [waf-global-rule-not-empty](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una regla de AWS WAF global contiene alguna condición. El control falla si no hay condiciones presentes en una regla.

Una regla de WAF global puede contener varias condiciones. Las condiciones de una regla permiten inspeccionar el tráfico y realizar una acción definida (permitir, bloquear o contar). Sin ninguna condición, el tráfico pasa sin inspección. Una regla de WAF global sin condiciones, pero con un nombre o etiqueta que sugiera permitir, bloquear o contar, podría llevar a suponer erróneamente que se está produciendo una de esas acciones.

Corrección

Para obtener instrucciones sobre cómo crear una regla y añadir condiciones, consulte [Creación de una regla y adición de condiciones](#) en la Guía para desarrolladores de AWS WAF .

Los grupos de reglas globales de [WAF.7] AWS WAF clásicos deben tener al menos una regla

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: AWS::WAF::RuleGroup

Regla de AWS Config : [waf-global-rulegroup-not-empty](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un grupo de reglas de AWS WAF globales tiene al menos una regla. El control falla si no hay reglas presentes en un grupo de reglas.

Un grupo de reglas globales de WAF puede contener varias reglas. Las condiciones de la regla permiten inspeccionar el tráfico y realizar una acción definida (permitir, bloquear o contar). Sin ninguna regla, el tráfico pasa sin inspección. Un grupo de reglas globales de la WAF sin reglas, pero con un nombre o etiqueta que sugiera permitir, bloquear o contar, podría llevar a suponer erróneamente que se está produciendo una de esas acciones.

Corrección

Para obtener instrucciones sobre cómo añadir una regla a un grupo de reglas, consulte [Creación de un grupo de reglas de AWS WAF clásico](#) en la Guía para AWS WAF desarrolladores de.

La web de [WAF.8] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas

Requisitos relacionados: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), (16), NIST.800-53.r5 SC-7 (21) NIST.800-53.r5 SC-7

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: AWS::WAF::WebACL

Regla de AWS Config : [waf-global-webacl-not-empty](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una ACL web de AWS WAF global contiene al menos una regla de WAF o un grupo de reglas de WAF. El control falla si una ACL web no contiene ninguna regla o grupo de reglas de WAF.

Una ACL web global de WAF puede contener una colección de reglas y grupos de reglas que inspeccionan y controlan las solicitudes web. Si una ACL web está vacía, el tráfico web puede pasar sin que el WAF lo detecte ni actúe en consecuencia, según la acción predeterminada.

Corrección

Para añadir reglas o grupos de reglas a una ACL web de AWS WAF global vacía, consulte [Edición de una ACL web](#) en la Guía para AWS WAF desarrolladores de. Para Filtrar, elija Global (CloudFront).

La AWS WAF web de [WAF.10] ACLs debe tener al menos una regla o grupo de reglas

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoría: Proteger - Configuración de red segura

Gravedad: media

Tipo de recurso: AWS::WAFv2::WebACL

Regla de AWS Config : [wafv2-webacl-not-empty](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una lista de control de acceso web (ACL web) de la AWS WAF V2 de contiene al menos una regla o un grupo de reglas. El control falla si una ACL web no contiene ninguna regla o grupo de reglas.

Una ACL web le proporciona un control detallado de todas las solicitudes web HTTP(S) a las que responde su recurso protegido. Una ACL web debe contener una colección de reglas y grupos de reglas que inspeccionen y controlen las solicitudes web. Si una ACL web está vacía, puede pasar el tráfico web sin detectarlo ni actuar en consecuencia, AWS WAF dependiendo de la acción predeterminada.

Corrección

Para añadir reglas o grupos de reglas a una ACL WAFV2 web vacía, consulte [Edición de una ACL web](#) en la Guía para AWS WAF desarrolladores de.

El registro de ACL AWS WAF web de [WAF.11] debe estar habilitado

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), (10), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (8), PCI DSS v4.0.1/10.4.2

Categoría: Identificar - Registro

Gravedad: baja

Tipo de recurso: AWS::WAFv2::WebACL

AWS Config regla: [wafv2-logging-enabled](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si el registro está activado para una lista de control de acceso web (ACL web) de la AWS WAF V2 de. Este control falla si el registro está desactivado para la ACL web.

Note

Este control no comprueba si el registro de ACL AWS WAF web está habilitado para una cuenta a través de Amazon Security Lake.

El registro mantiene la fiabilidad, la disponibilidad y el rendimiento de AWS WAF. Además, el registro es un requisito empresarial y de conformidad en muchas organizaciones. Al registrar el tráfico analizado por su ACL web, puede solucionar problemas de comportamiento de las aplicaciones.

Corrección

Para activar el registro de una ACL AWS WAF web, consulte [Administrar el registro de una ACL web en la Guía para AWS WAF](#) desarrolladores de.

AWS WAF Las reglas de [WAF.12] deben tener habilitadas las métricas CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), (10), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-7 NIST.800-53.r5 SC-7 (8), NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::WAFv2::RuleGroup

AWS Config regla: [wafv2-rulegroup-logging-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si una AWS WAF regla o un grupo de reglas de tienen habilitadas CloudWatch las métricas de Amazon. El control falla si la regla o el grupo de reglas no tienen habilitadas CloudWatch las métricas.

La configuración de las CloudWatch métricas de AWS WAF las reglas y los grupos de reglas proporciona visibilidad del flujo de tráfico. Puede ver qué reglas de ACL se activan y qué solicitudes se aceptan y bloquean. Esta visibilidad puede ayudarle a identificar actividades maliciosas en los recursos asociados.

Corrección

Para habilitar CloudWatch las métricas en un grupo de AWS WAF reglas, invoca la [UpdateRuleGroup](#) API. Para habilitar CloudWatch las métricas en una AWS WAF regla, invoca la API [UpdateWebACL](#). Establezca el campo `CloudWatchMetricsEnabled` como `true`. Cuando utiliza

la AWS WAF consola para crear reglas o grupos de reglas, CloudWatch las métricas se habilitan automáticamente.

Controles de Security Hub para WorkSpaces

Estos AWS Security Hub controles evalúan el WorkSpaces servicio y los recursos de Amazon.

Es posible que estos controles no estén disponibles en todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[WorkSpaces.1] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::WorkSpaces::Workspace

Regla de AWS Config : [workspaces-user-volume-encryption-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un volumen de usuarios de Amazon WorkSpaces Workspace está cifrado en reposo. El control falla si el volumen Workspace de usuarios no está cifrado en reposo.

Los datos en reposo hacen referencia a los datos que se almacenan en un almacenamiento persistente y no volátil durante cualquier periodo de tiempo. El cifrado de datos en reposo permite proteger la confidencialidad de los datos, lo que reduce el riesgo de que un usuario no autorizado pueda acceder a ellos.

Corrección

Para cifrar un volumen de WorkSpaces usuarios, consulte [Cifrar a Workspace en la Guía](#) de WorkSpaces administración de Amazon.

[WorkSpaces.2] los volúmenes WorkSpaces raíz deben cifrarse en reposo

Categoría: Proteger > Protección de datos > Cifrado de data-at-rest

Gravedad: media

Tipo de recurso: AWS::WorkSpaces::Workspace

Regla de AWS Config : [workspaces-root-volume-encryption-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un volumen raíz de Amazon WorkSpaces Workspace está cifrado en reposo. El control falla si el volumen Workspace raíz no está cifrado en reposo.

Los datos en reposo hacen referencia a los datos que se almacenan en un almacenamiento persistente y no volátil durante cualquier periodo de tiempo. El cifrado de datos en reposo permite proteger la confidencialidad de los datos, lo que reduce el riesgo de que un usuario no autorizado pueda acceder a ellos.

Corrección

Para cifrar un volumen WorkSpaces raíz, consulte [Cifrar a Workspace en la Guía](#) de WorkSpaces administración de Amazon.

Permisos necesarios para configurar los controles en Security Hub (CSPM)

Para ver información sobre los controles de seguridad y habilitar y deshabilitar los controles de seguridad en los estándares, la función AWS Identity and Access Management (IAM) que utiliza para acceder a AWS Security Hub Cloud Security Posture Management (CSPM) necesita permisos para realizar las siguientes operaciones de la API CSPM de Security Hub.

Para obtener los permisos necesarios, puede utilizar las políticas [gestionadas por CSPM de Security Hub](#). Como alternativa, puede actualizar las políticas de IAM personalizadas para incluir permisos para estas acciones.

- [BatchGetSecurityControls](#)— Devuelve información sobre un lote de controles de seguridad para la cuenta corriente y. Región de AWS
- [ListSecurityControlDefinitions](#): Devuelve información sobre los controles de seguridad que se aplican a un estándar específico.
- [ListStandardsControlAssociations](#): Identifica si un control de seguridad está activado o desactivado actualmente en cada uno de los estándares habilitados de la cuenta.
- [BatchGetStandardsControlAssociations](#): En el caso de un lote de controles de seguridad, identifica si cada control está actualmente activado o desactivado según un estándar específico.

- [BatchUpdateStandardsControlAssociations](#): Se utiliza para habilitar un control de seguridad en los estándares que incluyen el control, o para deshabilitar un control en los estándares. Se trata de un sustituto por lotes de la operación [UpdateStandardsControl](#) existente.
- [BatchUpdateStandardsControlAssociations](#): se utiliza para habilitar o deshabilitar un lote de controles de seguridad en los estándares que incluyen los controles. Se trata de un sustituto por lotes de la operación [UpdateStandardsControl](#) existente.
- [UpdateStandardsControl](#): se utiliza para habilitar o deshabilitar un único control de seguridad en los estándares que incluyen el control
- [DescribeStandardsControl](#): devuelve detalles sobre los controles de seguridad específicos.

Además de lo anterior APIs, debe añadir un permiso para llamar `BatchGetControlEvaluations` a su función de IAM. Este permiso es necesario para ver el estado de habilitación y conformidad de un control, el recuento de resultados de un control y la puntuación general de seguridad de los controles en la consola CSPM de Security Hub. Como solo se llama a la consola `BatchGetControlEvaluations`, este permiso no se corresponde directamente con el CSPM APIs o AWS CLI los comandos de Security Hub documentados públicamente.

Habilitación de controles en Security Hub (CSPM)

En AWS Security Hub Cloud Security Posture Management (CSPM), un control es una salvaguardia dentro de un estándar de seguridad que ayuda a una organización a proteger la confidencialidad, integridad y disponibilidad de su información. Cada control CSPM de Security Hub está relacionado con un recurso específico AWS . Cuando habilita un control, Security Hub CSPM comienza a ejecutar comprobaciones de seguridad para el control y genera resultados para él. El CSPM de Security Hub también tiene en cuenta todos los controles habilitados al calcular las puntuaciones de seguridad.

Puede elegir habilitar un control en todos los estándares de seguridad a los que se aplica. Como alternativa, puede configurar el estado de habilitación de forma diferente en los distintos estándares. Recomendamos la opción anterior, en la que el estado de habilitación de un control se alinea en todos los estándares habilitados. Para obtener instrucciones sobre cómo habilitar un control en todos los estándares a los que se aplica, consulte [Habilitación de un control en todos los estándares](#). Para obtener instrucciones sobre cómo habilitar un control en un estándar específico, consulte [Habilitación de un control en un estándar específico](#).

Si habilita la agregación entre regiones e inicia sesión en una región de agregación, la consola CSPM de Security Hub muestra los controles que están disponibles en al menos una región

vinculada. Si un control está disponible en una región vinculada, pero no en la región de agregación, no podrá habilitar ni deshabilitar ese control desde la región de agregación.

Puede habilitar y deshabilitar los controles en cada región mediante la consola CSPM de Security Hub, la API CSPM de Security Hub o. AWS CLI

Las instrucciones para habilitar y deshabilitar los controles varían en función de si se utiliza o no la [configuración centralizada](#). En este tema se describen las diferencias. La configuración central está disponible para los usuarios que integren Security Hub CSPM y. AWS Organizations Recomendamos utilizar la configuración centralizada para simplificar el proceso de habilitación y deshabilitación de los controles en entornos de varias cuentas y regiones. Si utiliza la configuración centralizada, puede habilitar un control en varias cuentas y regiones mediante el uso de políticas de configuración. Si no utiliza la configuración centralizada, debe habilitar un control por separado en cada cuenta y región.

Habilitación de un control en todos los estándares

Recomendamos habilitar el control de AWS la postura de seguridad (CSPM) de Security Hub Cloud en todos los estándares a los que se aplica el control. Si activa los resultados de control consolidados, recibirá un resultado por comprobación de control, incluso si un control pertenece a más de un estándar.

Habilitación entre estándares en entornos de varias cuentas y varias regiones

[Para habilitar el control de seguridad en varias Cuentas de AWS direcciones Regiones de AWS, debe iniciar sesión en la cuenta de administrador CSPM de Security Hub delegada y usar la configuración central.](#)

En la configuración central, el administrador delegado puede crear políticas de configuración CSPM de Security Hub que habiliten controles específicos en todos los estándares habilitados. A continuación, puede asociar la política de configuración a cuentas y unidades organizativas específicas (OUs) o a la raíz. La política de configuración entra en vigencia en su región de origen (también denominada región de agregación) y en todas las regiones vinculadas.

Las políticas de configuración pueden personalizarse. Por ejemplo, puede optar por habilitar todos los controles en una OU y puede optar por habilitar solo los controles de Amazon Elastic Compute Cloud (EC2) en otra OU. El nivel de granularidad depende de los objetivos previstos en materia de cobertura de seguridad en su organización. Para instrucciones sobre cómo crear una política de configuración que habilite controles especificados en estándares, consulte [Creación y asociación de políticas de configuración](#).

 Note

El administrador delegado puede crear políticas de configuración para administrar los controles en todos los estándares, excepto en el estándar de [administración de servicios](#). AWS Control Tower Los controles de este estándar deben configurarse en el servicio. AWS Control Tower

Si quiere que algunas cuentas configuren sus propios controles en lugar del administrador delegado, este puede designar esas cuentas como autoadministradas. Las cuentas autoadministradas deben configurar los controles por separado en cada región.

Habilitación entre estándares en una sola cuenta y región

Si no utiliza la configuración centralizada o tiene una cuenta autoadministrada, no podrá utilizar las políticas de configuración para habilitar de manera centralizada los controles en varias cuentas y regiones. Sin embargo, puede seguir estos pasos para habilitar un control en una sola cuenta y región.

Security Hub CSPM console

Para habilitar un control en los estándares en una cuenta y región

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Controles.
3. Seleccione la pestaña Deshabilitado.
4. Seleccione la opción situada junto a un control.
5. Seleccione Habilitar el control (esta opción no aparece en los controles que ya están activados).
6. Repítalo en cada región en la que quiere habilitar el control.

Security Hub CSPM API

Para habilitar un control en los estándares en una cuenta y región

1. Invoque la API [ListStandardsControlAssociations](#). Proporcione un ID de control de seguridad.

Ejemplo de solicitud:

```
{
  "SecurityControlId": "IAM.1"
}
```

2. Invoque la API [BatchUpdateStandardsControlAssociations](#). Proporcione el nombre de recurso de Amazon (ARN) de cualquier estándar en el que el control no esté habilitado. Para obtener el estándar ARNs, ejecute. [DescribeStandards](#)
3. Defina el parámetro AssociationStatus equivalente a ENABLED. Si sigue estos pasos para un control que ya está habilitado, la API devuelve una respuesta con el código de estado HTTP 200.

Ejemplo de solicitud:

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]
}
```

4. Repítalo en cada región en la que quiere habilitar el control.

AWS CLI

Para habilitar un control en los estándares en una cuenta y región

1. Ejecute el comando [list-standards-control-associations](#). Proporcione un ID de control de seguridad.

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Ejecute el comando [batch-update-standards-control-associations](#). Proporcione el nombre de recurso de Amazon (ARN) de cualquier estándar en el que el control no esté habilitado. Para obtener el estándar ARNs, ejecute el describe-standards comando.

- Defina el parámetro `AssociationStatus` equivalente a `ENABLED`. Si sigue estos pasos para un control que ya está habilitado, el comando devuelve una respuesta con el código de estado HTTP 200.

```
aws securityhub --region us-east-1 batch-update-standards-control-associations
--standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
"StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",
"StandardsArn": "arn:aws:securityhub::standards/cis-aws-foundations-benchmark/
v/1.4.0", "AssociationStatus": "ENABLED"}]'
```

- Repítalo en cada región en la que quiere habilitar el control.

Habilitación de un control en un estándar específico

Al habilitar un estándar en AWS Security Hub Cloud Security Posture Management (CSPM), todos los controles que se le aplican se habilitan automáticamente en ese estándar (con la excepción de los estándares administrados por servicios). Puede deshabilitar y rehabilitar controles específicos dentro del estándar. Sin embargo, recomendamos alinear el estado de habilitación de un control en todos los estándares habilitados. Para obtener instrucciones sobre cómo habilitar un control en todos los estándares, consulte [Habilitación de un control en todos los estándares](#).

La página de detalles de un estándar contiene la lista de los controles aplicables al estándar e información sobre los controles que están actualmente habilitados y deshabilitados en ese estándar.

En la página de detalles de los estándares, también puede habilitar controles en estándares específicos. Debe habilitar los controles en estándares específicos por separado en cada uno y. Cuenta de AWS Región de AWS Cuando habilita un control en estándares específicos, solo afecta a la cuenta y a la región actuales.

Para habilitar un control en un estándar, primero debe habilitar al menos un estándar al que se aplique el control. Para obtener instrucciones sobre cómo habilitar un estándar, consulte [Habilitación de un estándar de seguridad](#). Cuando habilita un control en uno o más estándares, Security Hub CSPM comienza a generar resultados para ese control. Security Hub CSPM incluye el [estado de control](#) en el cálculo de la puntuación de seguridad general y de las puntuaciones de seguridad estándar. Incluso si habilita un control en varios estándares, recibirá un único resultado por control de seguridad en todos los estándares si activa los resultados de control consolidados. Para obtener más información, consulte [Resultados de control consolidados](#).

Para habilitar un control en un estándar, el control debe estar disponible en su región actual. Para obtener más información, consulte [Disponibilidad de controles por región](#).

Siga estos pasos para habilitar el control CSPM de un Security Hub en un estándar específico. En lugar de los siguientes pasos, también puede usar la acción de la API de [UpdateStandardsControl](#) para habilitar los controles en un estándar específico. Para obtener instrucciones sobre cómo habilitar un control en todos los estándares, consulte [Habilitación entre estándares en una sola cuenta y región](#).

Security Hub CSPM console

Habilitación de un control en un estándar específico

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. Elija Estándares de seguridad en el panel de navegación.
3. Seleccione Ver resultados para el estándar correspondiente.
4. Seleccione un control.
5. Seleccione Habilitar el control (esta opción no aparece en los controles que ya están activados). Confirme seleccionando Habilitar.

Security Hub CSPM API

Habilitación de un control en un estándar específico

1. Ejecute [ListSecurityControlDefinitions](#) y proporcione un ARN estándar para obtener una lista de los controles disponibles para un estándar específico. Para obtener un ARN estándar, ejecute [DescribeStandards](#). Esta API devuelve un control de seguridad independiente del estándar, no un control IDs específico del estándar. IDs

Ejemplo de solicitud:

```
{
  "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
  best-practices/v/1.0.0"
}
```

2. Ejecute [ListStandardsControlAssociations](#) y proporcione un identificador de control específico para devolver el estado de activación actual de un control en cada estándar.

Ejemplo de solicitud:

```
{
  "SecurityControlId": "IAM.1"
}
```

3. Ejecute [BatchUpdateStandardsControlAssociations](#). Indique el ARN del estándar en el que desee habilitar el control.
4. Defina el parámetro AssociationStatus equivalente a ENABLED.

Ejemplo de solicitud:

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "ENABLED"}]
}
```

AWS CLI

Habilitación de un control en un estándar específico

1. Ejecute el comando [list-security-control-definitions](#) y proporcione un ARN estándar para obtener una lista de los controles disponibles para un estándar específico. Para obtener un ARN estándar, ejecute describe-standards. Este comando devuelve un control de seguridad independiente del estándar, no un control específico del estándar. IDs IDs

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1:standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Ejecute el comando [list-standards-control-associations](#) y proporcione un identificador de control específico para devolver el estado de habilitación actual de un control en cada estándar.

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Ejecute el comando [batch-update-standards-control-associations](#). Indique el ARN del estándar en el que desee habilitar el control.
4. Defina el parámetro AssociationStatus equivalente a ENABLED.

```
aws securityhub --region us-east-1 batch-update-standards-control-associations  
--standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",  
"StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-  
security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
```

Habilitación de nuevos controles en estándares habilitados automáticamente

AWS Security Hub Cloud Security Posture Management (CSPM) publica periódicamente nuevos controles y los añade a uno o más estándares. Puede elegir si quiere habilitar automáticamente nuevos controles en sus estándares habilitados.

Recomendamos utilizar la configuración central CSPM de Security Hub para activar automáticamente los nuevos controles de seguridad. Puede crear políticas de configuración que incluyan una lista de controles que se deben deshabilitar en los estándares. Todos los demás controles, incluidos los recién lanzados, están habilitados de manera predeterminada. Como alternativa, puede crear políticas que incluyan una lista de controles que se deben habilitar en los estándares. Todos los demás controles, incluidos los recién lanzados, están deshabilitados de manera predeterminada. Para obtener más información, consulte [Descripción de la configuración central en Security Hub \(CSPM\)](#).

Security Hub CSPM no habilita nuevos controles cuando se agregan a un estándar que usted no ha habilitado.

Las siguientes instrucciones solo se aplican si no utiliza la configuración centralizada.

Elija el método de acceso que prefiera y siga los pasos para activar automáticamente los nuevos controles en los estándares habilitados.

Note

Al activar automáticamente los nuevos controles siguiendo las instrucciones siguientes, podrá interactuar con los controles de la consola y de forma programática inmediatamente

después de soltarlos. Sin embargo, los controles activados automáticamente tienen el estado predeterminado temporal de Desactivado. Security Hub CSPM puede tardar varios días en procesar la liberación de control y designar el control como Habilitado en su cuenta. Durante el período de procesamiento, puede activar o desactivar manualmente un control, y Security Hub CSPM mantendrá esa designación independientemente de si tiene activada la activación automática del control.

Security Hub CSPM console

Habilitación automática de nuevos controles

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Configuración y luego elija la pestaña General.
3. En Controles, seleccione Editar.
4. Active la Activación automática de nuevos controles en los estándares habilitados.
5. Seleccione Save.

Security Hub CSPM API

Habilitación automática de nuevos controles

1. Ejecute [UpdateSecurityHubConfiguration](#).
2. Para activar automáticamente los nuevos controles para los estándares habilitados, establezca `AutoEnableControls` como `true`. Si no desea habilitar automáticamente los nuevos controles, establezca `AutoEnableControls` como `false`.

AWS CLI

Habilitación automática de nuevos controles

1. Ejecute el comando [update-security-hub-configuration](#).
2. Para activar automáticamente los nuevos controles para los estándares habilitados, especifique `--auto-enable-controls`. Si no desea habilitar automáticamente los nuevos controles, especifique `--no-auto-enable-controls`.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Comando de ejemplo:

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Si no habilita automáticamente los controles nuevos, debe habilitarlos manualmente. Para obtener instrucciones, consulte [Habilitación de controles en Security Hub \(CSPM\)](#).

Desactivación de los controles en Security Hub (CSPM)

Para reducir la presencia de ruido, puede resultar útil deshabilitar los controles que no sean relevantes para su entorno. En AWS Security Hub Cloud Security Posture Management (CSPM), puede deshabilitar un control en todos los estándares de seguridad o solo para estándares específicos.

Si deshabilita un control en todos los estándares, ocurre lo siguiente:

- Los controles de seguridad del control ya no se realizan.
- No se generan resultados adicionales para el control.
- Los hallazgos existentes del control se archivan automáticamente, normalmente en un plazo de 3 a 5 días, si se hace el mejor esfuerzo.
- Security Hub CSPM elimina todas AWS Config las reglas relacionadas que haya creado para el control.

Si deshabilita un control solo para estándares específicos, Security Hub CSPM deja de ejecutar comprobaciones de seguridad para el control solo para esos estándares. Esto también elimina el control de [los cálculos de la puntuación de seguridad](#) de cada uno de esos estándares. Si el control está habilitado en otros estándares, Security Hub CSPM conserva la AWS Config regla asociada, si corresponde, y continúa realizando comprobaciones de seguridad para el control de los demás estándares. Security Hub CSPM también incluye el control cuando calcula la puntuación de seguridad para cada uno de los demás estándares, lo que afecta a la puntuación de seguridad resumida.

Si deshabilita un estándar, todos los controles que se aplican al estándar se deshabilitan automáticamente para ese estándar. Sin embargo, es posible que los controles sigan activados en otros estándares. Al deshabilitar un estándar, Security Hub CSPM no rastrea qué controles se deshabilitaron para el estándar. Por lo tanto, si más adelante vuelve a activar el mismo estándar, todos los controles que se le aplican se habilitan automáticamente. Para obtener información acerca de la desactivación de un estándar, consulte [Desactivación de un estándar](#).

La desactivación de un control no es una acción permanente. Supongamos que deshabilita un control y, a continuación, habilita un estándar que incluye el control. A continuación, el control se habilita para ese estándar. Al habilitar un estándar en Security Hub CSPM, todos los controles que se aplican a ese estándar se habilitan automáticamente. Para obtener información sobre cómo habilitar un estándar, consulte [Habilitación de un estándar](#).

Temas

- [Deshabilitar un control en todos los estándares](#)
- [Deshabilitación de un control en un estándar específico](#)
- [Controles sugeridos para deshabilitar en Security Hub \(CSPM\)](#)

Deshabilitar un control en todos los estándares

Recomendamos deshabilitar el control de la postura AWS de seguridad (CSPM) en la nube de Security Hub en todos los estándares para mantener la alineación en toda la organización. Si deshabilita un control solo en estándares específicos, seguirá recibiendo información sobre el control si está habilitado en otros estándares.

Desactivación entre estándares en varias cuentas y regiones

Para deshabilitar un control de seguridad en varias Cuentas de AWS y Regiones de AWS, debe usar la [configuración central](#).

Cuando se utiliza la configuración central, el administrador delegado puede crear políticas de configuración CSPM de Security Hub que inhabiliten controles específicos en todos los estándares habilitados. A continuación, puede asociar la política de configuración a cuentas específicas o a la OUs raíz. La política de configuración entra en vigencia en su región de origen (también denominada región de agregación) y en todas las regiones vinculadas.

Las políticas de configuración pueden personalizarse. Por ejemplo, puede optar por deshabilitar todos los AWS CloudTrail controles de una unidad organizativa y puede optar por deshabilitar todos

los controles de IAM en otra unidad organizativa. El nivel de granularidad depende de los objetivos previstos en materia de cobertura de seguridad en su organización. Para instrucciones sobre cómo crear una política de configuración que deshabilite controles especificados en estándares, consulte [Creación y asociación de políticas de configuración](#).

 Note

El administrador delegado puede crear políticas de configuración para administrar los controles en todos los estándares, excepto en el estándar de administración de [servicios](#): [AWS Control Tower](#). Los controles de este estándar deben configurarse en el servicio. AWS Control Tower

Si quiere que algunas cuentas configuren sus propios controles en lugar del administrador delegado, este puede designar esas cuentas como autoadministradas. Las cuentas autoadministradas deben configurar los controles por separado en cada región.

Deshabilitación entre varios estándares en una sola cuenta y región

Si no utiliza la configuración centralizada o tiene una cuenta autoadministrada, no podrá utilizar las políticas de configuración para deshabilitar de manera centralizada los controles en varias cuentas y regiones. Sin embargo, puede deshabilitar un control en una sola cuenta y región.

Security Hub CSPM console

Deshabilitación de un control en los estándares en una cuenta y región

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Controles.
3. Seleccione la opción situada junto a un control.
4. Seleccione Desactivar el control. Esta opción no aparece en los controles que ya están deshabilitados.
5. Seleccione un motivo para deshabilitar el control y confírmelo seleccionando Deshabilitar.
6. Repítalo en cada región en la que quiere deshabilitar el control.

Security Hub CSPM API

Deshabilitación de un control en los estándares en una cuenta y región

1. Invoque la API [ListStandardsControlAssociations](#). Proporcione un ID de control de seguridad.

Ejemplo de solicitud:

```
{
  "SecurityControlId": "IAM.1"
}
```

2. Invoque la API [BatchUpdateStandardsControlAssociations](#). Proporcione el ARN de cualquier estándar en el que esté habilitado el control. Para obtener el estándar ARNs, ejecute [DescribeStandards](#).
3. Defina el parámetro AssociationStatus equivalente a DISABLED. Si sigue estos pasos para un control que ya está deshabilitado, la API devuelve una respuesta con el código de estado HTTP 200.

Ejemplo de solicitud:

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-
benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not
applicable to environment"}, {"SecurityControlId": "IAM.1", "StandardsArn":
"arn:aws:securityhub::standards/aws-foundational-security-best-practices/
v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
environment"}]}
}
```

4. Repítalo en cada región en la que quiere deshabilitar el control.

AWS CLI

Deshabilitación de un control en los estándares en una cuenta y región

1. Ejecute el comando [list-standards-control-associations](#). Proporcione un ID de control de seguridad.

```
aws securityhub --region us-east-1 list-standards-control-associations --  
security-control-id CloudTrail.1
```

2. Ejecute el comando [batch-update-standards-control-associations](#). Proporcione el ARN de cualquier estándar en el que esté habilitado el control. Para obtener el estándar ARNs, ejecute el `describe-standards` comando.
3. Defina el parámetro `AssociationStatus` equivalente a `DISABLED`. Si sigue estos pasos para un control que ya está deshabilitado, el comando devuelve una respuesta con el código de estado HTTP 200.

```
aws securityhub --region us-east-1 batch-update-standards-control-associations  
--standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",  
"StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/  
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable  
to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":  
"arn:aws:securityhub::standards/cis-aws-foundations-benchmark/v/1.4.0",  
"AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to  
environment"}]'
```

4. Repítalo en cada región en la que quiere deshabilitar el control.

Deshabilitación de un control en un estándar específico

Puede deshabilitar un control solo en estándares de seguridad específicos, en lugar de en todos los estándares. Si el control se aplica a otros estándares habilitados, AWS Security Hub Cloud Security Posture Management (CSPM) seguirá realizando comprobaciones de seguridad para el control y usted seguirá recibiendo los resultados del control.

Sin embargo, recomendamos alinear el estado de habilitación de un control en todos los estándares habilitados a los que se aplica el control. Para obtener información sobre cómo deshabilitar un control en todos los estándares a los que se aplica, consulte [Deshabilitar un control en todos los estándares](#)

En la página de detalles de los estándares, también puede desactivar los controles de un estándar específico. Debe deshabilitar los controles de normas específicas por separado en cada una Cuenta de AWS y Región de AWS. Al deshabilitar un control en normas específicas, solo afecta a la cuenta corriente y a la región.

Elija el método que prefiera y siga estos pasos para deshabilitar un control en uno o más estándares específicos.

Security Hub CSPM console

Deshabilitación de un control en un estándar específico

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
2. Elija Estándares de seguridad en el panel de navegación. Seleccione Ver resultados para el estándar correspondiente.
3. Seleccione un control.
4. Seleccione Desactivar el control. Esta opción no aparece en los controles que ya están deshabilitados.
5. Indique el motivo para deshabilitar el control y confirme seleccionando Deshabilitar.

Security Hub CSPM API

Deshabilitación de un control en un estándar específico

1. Ejecute [ListSecurityControlDefinitions](#) y proporcione un ARN estándar para obtener una lista de los controles disponibles para un estándar específico. Para obtener un ARN estándar, ejecute [DescribeStandards](#). Esta API devuelve un control de seguridad independiente del estándar IDs, no un control específico del estándar. IDs

Ejemplo de solicitud:

```
{
  "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-best-practices/v/1.0.0"
}
```

2. Ejecute [ListStandardsControlAssociations](#) y proporcione un identificador de control específico para devolver el estado de activación actual de un control en cada estándar.

Ejemplo de solicitud:

```
{
  "SecurityControlId": "IAM.1"
}
```

}

3. Ejecute [BatchUpdateStandardsControlAssociations](#). Proporcione el ARN del estándar en el que desea deshabilitar el control.
4. Defina el parámetro `AssociationStatus` equivalente a `DISABLED`. Si sigue estos pasos para un control que ya está deshabilitado, la API devuelve una respuesta con el código de estado HTTP 200.

Ejemplo de solicitud:

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to environment"}]
}
```

AWS CLI

Deshabilitación de un control en un estándar específico

1. Ejecute el comando [list-security-control-definitions](#) y proporcione un ARN estándar para obtener una lista de los controles disponibles para un estándar específico. Para obtener un ARN estándar, ejecute `describe-standards`. Este comando devuelve un control de seguridad independiente del estándar, no un control específico del estándar. IDs

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Ejecute el comando [list-standards-control-associations](#) y proporcione un identificador de control específico para devolver el estado de habilitación actual de un control en cada estándar.

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```


3. Ejecute el comando [batch-update-standards-control-associations](#). Proporcione el ARN del estándar en el que desea deshabilitar el control.
4. Defina el parámetro AssociationStatus equivalente a DISABLED. Si sigue estos pasos para un control que ya está habilitado, el comando devuelve una respuesta con el código de estado HTTP 200.

```
aws securityhub --region us-east-1 batch-update-standards-control-associations --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to environment"}]'
```

Controles sugeridos para deshabilitar en Security Hub (CSPM)

Recomendamos deshabilitar algunos controles de gestión de AWS la postura de seguridad (CSPM) de Security Hub Cloud para reducir el ruido de búsqueda y los costes de uso.

Controles que utilizan recursos globales

Algunos son Servicios de AWS compatibles con recursos globales, lo que significa que puede acceder al recurso desde cualquier lugar. Región de AWS Para ahorrar costes AWS Config, puedes desactivar el registro de los recursos globales en todas las regiones excepto en una. Sin embargo, una vez hecho esto, Security Hub CSPM seguirá realizando comprobaciones de seguridad en todas las regiones en las que haya un control activado y le cobrará en función del número de comprobaciones por cuenta y región. En consecuencia, para reducir el ruido de búsqueda y ahorrar en el coste del Security Hub CSPM, también debe deshabilitar los controles que implican recursos globales en todas las regiones, excepto en la región que registra los recursos globales.

Si un control incluye recursos globales, pero solo está disponible en una región, si lo deshabilita en esa región, no podrá obtener resultados para el recurso subyacente. En ese caso, recomendamos que mantenga el control habilitado. Al utilizar la agregación entre regiones, la región en la que esté disponible el control debe ser la región de agregación o una de las regiones vinculadas. Los siguientes controles incluyen recursos globales, pero solo están disponibles en una sola región:

- Todos los CloudFront controles: disponibles solo en la región EE.UU. Este (Norte de Virginia)
- GlobalAccelerator.1 — Disponible solo en la región EE.UU. Oeste (Oregón)
- Ruta 53.2: disponible solo en la región EE.UU. Este (Norte de Virginia)

- WAF.1, WAF.6, WAF.7, WAF.8: disponibles solo en la región EE.UU. Este (Norte de Virginia)

Note

Si usa la configuración central, Security Hub CSPM deshabilita automáticamente los controles que involucran recursos globales en todas las regiones, excepto en la región de origen. Los controles que elija habilitar a través de una política de configuración están habilitados en todas las regiones en las que están disponibles. Para limitar las búsquedas de estos controles a una sola región, puede actualizar la configuración de la AWS Config grabadora y desactivar el registro de recursos globales en todas las regiones, excepto en la región de origen.

Si un control habilitado que implica recursos globales no es compatible en la región de origen, Security Hub CSPM intenta habilitar el control en una región vinculada en la que se admita el control. Con la configuración central, no hay cobertura para un control que no está disponible en la región de origen ni en ninguna de las regiones vinculadas.

Para obtener más información acerca de la configuración centralizada, consulte [Descripción de la configuración central en Security Hub \(CSPM\)](#).

Para los controles que tienen un tipo de programación periódica, es necesario deshabilitarlos en Security Hub CSPM para evitar la facturación. Si se establece el AWS Config parámetro `includeGlobalResourceTypes` en, `false` no se ven afectados los controles periódicos de CSPM de Security Hub.

Los siguientes controles CSPM de Security Hub utilizan recursos globales:

- [\[Cuenta.1\] La información de contacto de seguridad debe proporcionarse para un Cuenta de AWS](#)
- [\[Account.2\] Cuentas de AWS debe formar parte de una organización AWS Organizations](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)

- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)
- [\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)
- [\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)
- [\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)
- [\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)
- [\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)
- [\[IAM.7\] Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)
- [\[IAM.10\] Las políticas de contraseñas de usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.11\] Asegurar que la política de contraseñas de IAM requiera al menos una letra mayúscula](#)
- [\[IAM.12\] Asegurar que la política de contraseñas de IAM requiera al menos una letra minúscula](#)
- [\[IAM.13\] Asegurar que la política de contraseñas de IAM requiera al menos un símbolo](#)
- [\[IAM.14\] Asegurar que la política de contraseñas de IAM requiera al menos un número](#)
- [\[IAM.15\] Asegurar que la política de contraseñas de IAM requiera una longitud mínima de 14 o más](#)
- [\[IAM.16\] Asegurar que la política de contraseñas de IAM impida la reutilización de contraseñas](#)
- [\[IAM.17\] Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos](#)
- [\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)
- [\[IAM.19\] MFA se debe habilitar para todos los usuarios de IAM](#)

- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)
- [\[IAM.22\] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días](#)
- [\[IAM.24\] Los roles de IAM deben etiquetarse](#)
- [\[IAM.25\] Los usuarios de IAM deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IAM.27\] Las identidades de IAM no deben tener adjunta la política AWSCloud ShellFullAccess](#)
- [\[KMS.1\] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.2\] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

CloudTrail controles de registro

Este control trata del uso de AWS Key Management Service (AWS KMS) para cifrar los registros de AWS CloudTrail seguimiento. Si registra estos registros en una cuenta de registro centralizada, debe habilitar este control solo en la cuenta y la región en las que se realiza el registro centralizado.

Note

Si utiliza la [configuración centralizada](#), el estado de habilitación de un control se alinea en la región de origen y en las regiones vinculadas. No puede deshabilitar un control en algunas regiones y habilitarlo en otras. En este caso, suprima los resultados de los siguientes controles para reducir el ruido de los resultados.

- [\[CloudTrail.2\] CloudTrail debe tener habilitado el cifrado en reposo](#)

CloudWatch controles de alarma

Si prefieres utilizar Amazon GuardDuty para la detección de anomalías en lugar de CloudWatch las alarmas de Amazon, puedes desactivar los siguientes controles, que se centran en CloudWatch las alarmas:

- [\[CloudWatch.1\] Debe existir un filtro de métricas de registro y una alarma para el uso del usuario «raíz»](#)
- [\[CloudWatch.2\] Asegurar que haya un filtro de métricas de registro y alarma para las llamadas a la API no autorizadas](#)
- [\[CloudWatch.3\] Asegurar que haya un filtro de métricas de registro y alarma de registro para el inicio de sesión en la Consola de administración sin MFA](#)
- [\[CloudWatch.4\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de IAM](#)
- [\[CloudWatch.5\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de CloudTrail configuración de](#)
- [\[CloudWatch.6\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los errores de AWS Management Console autenticación](#)
- [\[CloudWatch.7\] Asegurar que haya un filtro de métricas de registro y alarma de registro para la deshabilitación o eliminación programada de claves administradas por el cliente](#)
- [\[CloudWatch.8\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de bucket de S3](#)
- [\[CloudWatch.9\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de AWS Config configuración de](#)
- [\[CloudWatch.10\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de grupos de seguridad](#)
- [\[CloudWatch.11\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios en las listas de control de acceso a la red \(NACL\)](#)
- [\[CloudWatch.12\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a las puertas de enlace de la red](#)
- [\[CloudWatch.13\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios ala tabla de enrutamiento](#)
- [\[CloudWatch.14\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de VPC](#)

Descripción de los controles de seguridad y las puntuaciones en Security Hub (CSPM)

Para cada control que habilite, AWS Security Hub Cloud Security Posture Management (CSPM) ejecuta comprobaciones de seguridad. Una comprobación de seguridad produce un resultado que indica si un AWS recurso específico cumple con las reglas que incluye el control.

Algunas comprobaciones se ejecutan de forma periódica. Otras comprobaciones solo se ejecutan cuando se produce un cambio en el estado del recurso. Para obtener más información, consulte [Programación para ejecutar comprobaciones de seguridad](#).

Muchas comprobaciones de seguridad utilizan reglas AWS Config administradas o personalizadas para establecer los requisitos de conformidad. Para ejecutar estas comprobaciones, debe configurar AWS Config y activar el registro de recursos para los recursos necesarios. Para obtener más información sobre la configuración AWS Config, consulte [Habilitación y configuración AWS Config de Security Hub CSPM](#). Para obtener una lista de AWS Config los recursos que debe registrar para cada norma, consulte [AWS Config Recursos necesarios para los hallazgos de control](#). Otros controles utilizan funciones Lambda personalizadas, que son administradas por Security Hub CSPM y no requieren ningún requisito previo.

A medida que Security Hub CSPM ejecuta las comprobaciones de seguridad, genera hallazgos y les asigna un estado de conformidad. Para obtener más información sobre el estado de conformidad, consulte [Evaluación del estado de cumplimiento de las conclusiones del CSPM de Security Hub](#).

Security Hub CSPM utiliza el estado de conformidad de los hallazgos de control para determinar un estado de control general. En función del estado del control, Security Hub CSPM también calcula una puntuación de seguridad para todos los controles habilitados y para estándares específicos. Para obtener más información, consulte [the section called “Estado de conformidad y el estado de control”](#) y [the section called “Calcular las puntuaciones de seguridad”](#).

Si ha activado los hallazgos de control consolidados, Security Hub CSPM genera un único hallazgo incluso cuando un control está asociado a más de un estándar. Para obtener más información, consulte [Resultados de control consolidados](#).

Temas

- [AWS Config Recursos necesarios para los hallazgos de control](#)
- [Programación para ejecutar comprobaciones de seguridad](#)
- [Generación y actualización de los resultados de control](#)

- [Evaluación del estado de cumplimiento y el estado de control](#)
- [Calcular las puntuaciones de seguridad](#)

AWS Config Recursos necesarios para los hallazgos de control

En AWS Security Hub Cloud Security Posture Management (CSPM), algunos controles utilizan AWS Config reglas vinculadas a servicios que detectan cambios de configuración en los recursos. Para que Security Hub CSPM genere resultados precisos para estos controles, debe habilitar AWS Config y activar el registro de recursos en AWS Config. Para obtener información sobre cómo Security Hub CSPM usa AWS Config las reglas y cómo habilitarlas y configurarlas en AWS Config, consulte [Habilitación y configuración AWS Config de Security Hub CSPM](#). Para obtener información detallada sobre el registro de recursos, consulte [Trabajar con la grabadora de configuración](#) en la Guía AWS Config para desarrolladores.

Para obtener resultados de control precisos, debe activar el registro de AWS Config recursos para los controles habilitados con un tipo de programa activado por cambios. Algunos controles con un tipo de programación periódica también requieren el registro de recursos. En esta página se enumeran los recursos necesarios para estos controles CSPM de Security Hub.

Los controles CSPM de Security Hub pueden basarse en AWS Config reglas administradas o reglas CSPM personalizadas de Security Hub. Asegúrese de que no haya políticas AWS Identity and Access Management (de IAM) o políticas AWS Organizations administradas que impidan tener AWS Config permiso para registrar sus recursos. Los controles CSPM de Security Hub evalúan las configuraciones de los recursos directamente y no tienen en cuenta AWS Organizations las políticas.

Note

Si una región de AWS para un control no está disponible, el recurso correspondiente no está disponible en AWS Config. Para obtener una lista de estos límites, consulte [Límites regionales de los controles CSPM de Security Hub](#).

Temas

- [Recursos necesarios para todos los controles CSPM de Security Hub](#)
- [Recursos necesarios para el estándar AWS fundamental de mejores prácticas de seguridad](#)
- [Recursos necesarios para el índice de referencia de las AWS fundaciones de la CEI](#)

- [Recursos necesarios para la norma NIST SP 800-53, revisión 5](#)
- [Recursos necesarios para la norma NIST SP 800-171, revisión 2](#)
- [Recursos necesarios para PCI DSS v3.2.1](#)
- [Recursos necesarios para el estándar de etiquetado AWS de recursos](#)
- [Recursos necesarios para el estándar de gestión de AWS Control Tower servicios](#)

Recursos necesarios para todos los controles CSPM de Security Hub

Para que Security Hub CSPM genere resultados para los controles activados por cambios que estén habilitados y usen una AWS Config regla, debe registrar los siguientes tipos de recursos en AWS Config. En esta tabla también se indican los controles que evalúan un tipo concreto de recurso. Un único control puede evaluar más de un tipo de recurso.

Servicio de AWS	Tipos de recurso	Controles relacionados
AWS Amplify	AWS::Amplify::App	Amplificar.1
	AWS::Amplify::Branch	Amplificar.2
Amazon API Gateway	AWS::ApiGateway::Stage	APIGateway1. APIGateway2. APIGateway3. APIGateway4. APIGateway5.
	AWS::ApiGatewayV2::Stage	APIGateway1. APIGateway9.
AWS AppConfig	AWS::AppConfig::Application	AppConfig1.

Servicio de AWS	Tipos de recurso	Controles relacionados
	AWS::AppConfig::ConfigurationProfile	AppConfig2.
	AWS::AppConfig::Environment	AppConfig3.
	AWS::AppConfig::ExtensionAssociation	AppConfig4.
Amazon AppFlow	AWS::AppFlow::Flow	AppFlow1.
AWS App Runner	AWS::AppRunner::Service	AppRunner1.
	AWS::AppRunner::VpcConnector	AppRunner2.
AWS AppSync	AWS::AppSync::GraphQLApi	AppSync2. AppSync4. AppSync5.
	AWS::AppSync::ApiCache	AppSync1. AppSync6.
AWS Backup	AWS::Backup::BackupPlan	Backup.5

Servicio de AWS	Tipos de recurso	Controles relacionados
	AWS::Backup::BackupVault	Backup.3
	AWS::Backup::RecoveryPoint	Backup.1 Backup.2
	AWS::Backup::ReportPlan	Backup.4
AWS Batch	AWS::Batch::ComputeEnvironment	Lote 3 Lote 4.
	AWS::Batch::JobQueue	Lote.1
	AWS::Batch::SchedulingPolicy	Lote 2.
AWS Certificate Manager (ACM)	AWS::ACM::Certificate	ACM.1 ACM.2 ACM.3
Amazon Athena	AWS::Athena::DataCatalog	Athena.2
	AWS::Athena::WorkGroup	Athena.3 Athena.4

Servicio de AWS	Tipos de recurso	Controles relacionados
AWS CloudFormation	AWS::CloudFormation::Stack	CloudFormation2.
Amazon CloudFront	AWS::CloudFront::Distribution	CloudFront1. CloudFront3. CloudFront4. CloudFront5. CloudFront6. CloudFront.7. CloudFront.8. CloudFront.9. CloudFront.10 CloudFront.13 CloudFront.14
AWS CloudTrail	AWS::CloudTrail::Trail	CloudTrail9.
Amazon CloudWatch	AWS::CloudWatch::Alarm	CloudWatch.15 CloudWatch.17
AWS CodeArtifact	AWS::CodeArtifact::Repository	CodeArtifact1.

Servicio de AWS	Tipos de recurso	Controles relacionados
AWS CodeBuild	AWS::CodeBuild::Project	CodeBuild1. CodeBuild2. CodeBuild3. CodeBuild4.
	AWS::CodeBuild::ReportGroup	CodeBuild.7.
Amazon CodeGuru Profiler	AWS::CodeGuruProfiler::ProfilingGroup	CodeGuruProfiler1.
CodeGuru Revisor de Amazon	AWS::CodeGuruReviewer::RepositoryAssociation	CodeGuruReviewer1.
Amazon Cognito	AWS::Cognito::UserPool	Cognito.1
Amazon Connect	AWS::CustomerProfiles::ObjectType	Conectar.1
	AWS::Connect::Instance	Conectar.2
AWS DataSync	AWS::DataSync::Task	DataSync1. DataSync2.

Servicio de AWS	Tipos de recurso	Controles relacionados
Amazon Detective	AWS::Detective::Graph	Detective.1
AWS Database Migration Service (AWS DMS)	AWS::DMS::Certificate	DMS.2
	AWS::DMS::Endpoint	DMS.9
		DMS.10
		DMS.11
		DMS.12
	AWS::DMS::EventSubscription	DMS.3
	AWS::DMS::ReplicationInstance	DMS.4
		DMS.6
	AWS::DMS::ReplicationSubnetGroup	DMS.5
	AWS::DMS::ReplicationTask	DMS.7
		DMS.8
Amazon DynamoDB	AWS::DynamoDB::Table	DynamoDB.1
		DynamoDB.2
		DynamoDB.5
		DynamoDB.6

Servicio de AWS	Tipos de recurso	Controles relacionados
Amazon Elastic Compute Cloud (EC2)	AWS::EC2:ClientVpnEndpoint	EC2.1
	AWS::EC2:CustomerGateway	EC2.36
	AWS::EC2:DHCPOptions	EC2.174
	AWS::EC2::EIP	EC2.12
		EC2.37
	AWS::EC2:FlowLog	EC2.48
	AWS::EC2:Instance	EC2.4.
		EC2.8.
		EC2.9.
		EC2.17
		EC2.24
		EC2.38
		EMR.1
		SSM.1
	AWS::EC2:InternetGateway	EC2.39

Servicio de AWS	Tipos de recurso	Controles relacionados
	AWS::EC2: :LaunchTemplate	EC2.25 EC2.170 EC2.175
	AWS::EC2: :NatGateway	EC2.40
	AWS::EC2: :NetworkAcl	EC2.16 EC2.21 EC2.41
	AWS::EC2: :NetworkInterface	EC2.22 EC2.35
	AWS::EC2: :PrefixList	EC2.176
	AWS::EC2: :RouteTable	EC2.42
	AWS::EC2: :SecurityGroup	EC2.2. EC2.13 EC2.14 EC2.18 EC2.19 EC2.43
	AWS::EC2: :SpotFleet	EC2.173

Servicio de AWS	Tipos de recurso	Controles relacionados
	AWS::EC2: :Subnet	EC2.15 EC2.44 ElastiCache.7.
	AWS::EC2: :TrafficMirrorFilter	EC2.178
	AWS::EC2: :TrafficMirrorSession	EC2.177
	AWS::EC2: :TrafficMirrorTarget	EC2.179
	AWS::EC2: :TransitGateway	EC2.23 EC2.52
	AWS::EC2: :TransitGatewayAttachment	EC2.33
	AWS::EC2: :TransitGatewayRouteTable	EC2.34
	AWS::EC2: :Volume	EC2.3. EC2.45

Servicio de AWS	Tipos de recurso	Controles relacionados
	AWS::EC2::VPC	EC2.6. EC2.46
	AWS::EC2::VPCBlockPublicAccessOptions	EC2.172
	AWS::EC2::VPCEndpointService	EC2.47
	AWS::EC2::VPCPeeringConnection	EC2.49
	AWS::EC2::VPNConnection	EC2.20 EC2.171
	AWS::EC2::VPNGateway	EC2.50
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup	AutoScaling1. AutoScaling2. AutoScaling6. AutoScaling.9. AutoScaling.10
	AWS::AutoScaling::LaunchConfiguration	AutoScaling3. Autoscaling.5

Servicio de AWS	Tipos de recurso	Controles relacionados
Amazon EC2 Systems Manager (SSM)	AWS::SSM: :AssociationCompliance	SSM.3
	AWS::SSM: :ManagedInstanceInventory	SSM.1
	AWS::SSM: :PatchCompliance	SSM.2
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR: :PublicRepository	ECR.4
	AWS::ECR: :Repository	ECR.2 ECR.3 ECR.5
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS: :Cluster	EC.12 ECS.14
	AWS::ECS: :Service	ECS.2 ECS.10 ECS.13

Servicio de AWS	Tipos de recurso	Controles relacionados
	AWS::ECS: :TaskDefinition	ECS.1
		ECS.3
		ECS.4
		ECS.5
		ECS.8
		ECS.9
		ECS.15
		ECS.17
Amazon Elastic File System (Amazon EFS)	AWS::ECS: :TaskSet	ECS.16
	AWS::EFS: :AccessPoint	EFS.3
		EFS.4
		EFS.5
	AWS::EFS: :FileSystem	EFS.7
		EFS.8
Amazon Elastic Kubernetes Service (Amazon EKS)	AWS::EKS: :Cluster	EKS.2
		EKS.6
		EKS.8
	AWS::EKS: :IdentityProviderConfig	EKS.7

Servicio de AWS	Tipos de recurso	Controles relacionados
AWS Elastic Beanstalk	AWS::ElasticBeanstalk::Environment	ElasticBeanstalk1. ElasticBeanstalk2. ElasticBeanstalk3.
Elastic Load Balancing	AWS::ElasticLoadBalancing::LoadBalancer	ELB.2
		ELB.3
		ELB.5
		ELB.7
		ELB.8
		ELB.9
		ELB.10
		ELB.14
	AWS::ElasticLoadBalancingV2::Listener	ELB.17
	AWS::ElasticLoadBalancingV2::LoadBalancer	ELB.1
		ELB.4
		ELB.5
		ELB.6
		ELB.12
		ELB.13
		ELB.16

Servicio de AWS	Tipos de recurso	Controles relacionados
ElasticSearch	AWS::Elasticsearch::Domain	ES.3
		ES.4
		ES.5
		ES.6
		ES.7
		ES.8
		ES.9
Amazon EMR	AWS::EMR::SecurityConfiguration	EMR.3 EMR.4
Amazon EventBridge	AWS::Events::EventBus	EventBridge2. EventBridge3.
	AWS::Events::Endpoint	EventBridge4.
Amazon Fraud Detector	AWS::FraudDetector::EntityType	FraudDetector1.
	AWS::FraudDetector::Label	FraudDetector2.
	AWS::FraudDetector::Outcome	FraudDetector3.

Servicio de AWS	Tipos de recurso	Controles relacionados
	AWS::FraudDetector::Variable	FraudDetector4.
AWS Global Accelerator	AWS::GlobalAccelerator::Accelerator	GlobalAccelerator1.
AWS Glue	AWS::Glue::Job	Glue.1 Pegamento.4
	AWS::Glue::MLTransform	Glue.3
Amazon GuardDuty	AWS::GuardDuty::Detector	GuardDuty4.
	AWS::GuardDuty::Filter	GuardDuty2.
	AWS::GuardDuty::IPSet	GuardDuty3.
AWS Identity and Access Management (IAM)	AWS::IAM::Group	IAM.27 KMS.2
	AWS::IAM::Policy	IAM.1 IAM.21 KMS.1

Servicio de AWS	Tipos de recurso	Controles relacionados
	AWS::IAM::Role	IAM.24
		IAM.27
		KMS.2
	AWS::IAM::User	IAM.2
		IAM.3
		IAM.5
		IAM.8
		IAM.19
		IAM.22
		IAM.25
		IAM.27
		KMS.2
AWS Identity and Access Management Access Analyzer	AWS::AccessAnalyzer::Analyzer	IAM.23
Amazon Interactive Video Service (Amazon IVS)	AWS::IVS::PlaybackKeyPair	IVS.1
	AWS::IVS::RecordingConfiguration	IVS.2
	AWS::IVS::Channel	IVS.3

Servicio de AWS	Tipos de recurso	Controles relacionados
AWS IoT	AWS::IoT: :Authorizer	IoT.4
	AWS::IoT: :Dimension	IoT.3
	AWS::IoT: :MitigationAction	IoT.2
	AWS::IoT: :Policy	IoT.6
	AWS::IoT: :RoleAlias	IoT.5
	AWS::IoT: :SecurityProfile	IoT.1
AWS Eventos de IoT	AWS::IoTEvents::AlarmModel	IoT TEEvents 1.3
	AWS::IoTEvents::DetectorModel	IoT TEEvents 3.2
	AWS::IoTEvents::Input	IoT TEEvents 1.1
AWS IoT SiteWise	AWS::IoTSiteWise::AssetModel	IoT Site Wise.1

Servicio de AWS	Tipos de recurso	Controles relacionados
	AWS::IoTSiteWise::Dashboard	Io Wise.2 TSite
	AWS::IoTSiteWise::Gateway	Io Wise.3 TSite
	AWS::IoTSiteWise::Portal	Io Wise.4 TSite
	AWS::IoTSiteWise::Project	Io TSite Wise.5
AWS IoT TwinMaker	AWS::IoTThingMaker::Entity	TTwinIo Maker. 4
	AWS::IoTThingMaker::Scene	Io TTwin Maker.3
	AWS::IoTThingMaker::SyncJob	Io Maker.1 TTwin
	AWS::IoTThingMaker::Workspace	Io Maker.2 TTwin
AWS IoT Wireless	AWS::IoTWireless::MulticastGroup	IoT TWireless 1.1

Servicio de AWS	Tipos de recurso	Controles relacionados
	AWS::IoTWireless::ServiceProfile	IoTWireless 1.2
	AWS::IoTWireless::FleetTask	IoTWireless 1.3
Amazon Keyspaces (para Apache Cassandra)	AWS::Cassandra::Keyspace	Espacios clave. 1
Amazon Kinesis	AWS::Kinesis::Stream	Kinesis.1
		Kinesis.2
		Kinesis.3
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias	S3.17
	AWS::KMS::Key	KMS.3
		KMS.5
		S3.17
AWS Lambda	AWS::Lambda::Function	Lambda.1
		Lambda.2
		Lambda.3
		Lambda.5
		Lambda.6
Amazon MSK	AWS::MSK::Cluster	MSK.1
		MSK.2

Servicio de AWS	Tipos de recurso	Controles relacionados
Amazon MQ	AWS::KafkaConnect:Connector	MSK.3
	AWS::AmazonMQ::Broker	MQ.2
		MQ.3
		MQ.4
		MQ.5
AWS Network Firewall	AWS::NetworkFirewall::Firewall	NetworkFirewall1.
		NetworkFirewall7.
		NetworkFirewall.9.
		NetworkFirewall.10
	AWS::NetworkFirewall::FirewallPolicy	NetworkFirewall3.
		NetworkFirewall4.
		NetworkFirewall5.
	AWS::NetworkFirewall::RuleGroup	NetworkFirewall.8.
		NetworkFirewall6.

Servicio de AWS	Tipos de recurso	Controles relacionados
OpenSearch Servicio Amazon	AWS::OpenSearch::Domain	OpenSearch.1 OpenSearch.2 Opensearch.3 Opensearch.4 Opensearch.5 Opensearch.6 Opensearch.7 Opensearch.8 Opensearch.9 Opensearch.10 Opensearch.11
AWS Private CA	AWS::ACMPCA::CertificateAuthority	PCA.2

Servicio de AWS	Tipos de recurso	Controles relacionados
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster	DocumentDB.1
		DocumentDB.2
		DocumentDB.4
		DocumentDB.5
		Neptune.1
		Neptune.2
		Neptune.4
		Neptune.5
		Neptune.7
		Neptune.8
		Neptune.9
		RDS.7
		RDS.12
		RDS.14
		RDS.15
		RDS.16
		RDS.24
		RDS.27
		RDS.28
		RDS.34
		RDS.35

Servicio de AWS	Tipos de recurso	Controles relacionados
		RDS.37
	AWS::RDS: :DBClusterSnapshot	DocumentDB.3
		Neptune.3
		Neptune.6
		RDS.1
		RDS.4
		RDS.29

Servicio de AWS	Tipos de recurso	Controles relacionados
	AWS::RDS: DBInstance	RDS.2
		RDS.3
		RDS.5
		RDS.6
		RDS.8
		RDS.9
		RDS.10
		RDS.11
		RDS.13
		RDS.17
		RDS.18
		RDS.23
		RDS.25
		RDS.30
		RDS.36
		RDS.40
	AWS::RDS: DBSecurityGroup	RDS.31

Servicio de AWS	Tipos de recurso	Controles relacionados
	AWS::RDS: :DBSnapshot	RDS.1
		RDS.4
		RDS.32
	AWS::RDS: :DBSubnetGroup	RDS.33
	AWS::RDS: :EventSubscription	RDS.19
		RDS.20
		RDS.21
		RDS.22
Amazon Redshift	AWS::Redshift::Cluster	Redshift.1
		Redshift.2
		Redshift.3
		Redshift.4
		Redshift.6
		Redshift.7
		Redshift.8
		Redshift.9
		Redshift.10
		Redshift.11

Servicio de AWS	Tipos de recurso	Controles relacionados
	AWS::Redshift::ClusterParameterGroup	Redshift.2 Redshift. 17
	AWS::Redshift::ClusterSnapshot	Redshift.13
	AWS::Redshift::ClusterSubnetGroup	Redshift.14 Redshift. 16
	AWS::Redshift::EventSubscription	Redshift.12
Amazon Route 53	AWS::Route53::HostedZone	Route53.2
	AWS::Route53::HealthCheck	Route53.1
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccessPoint	S3.19
	AWS::S3::AccountPublicAccessBlock	S3.2 S3.3

Servicio de AWS	Tipos de recurso	Controles relacionados
	AWS::S3::Bucket	CloudTrail6.
		CloudTrail7.
		S3.2
		S3.3
		S3.5
		S3.6
		S3.7
		S3.8
		S3.9
		S3.10
		S3.11
		S3.12
		S3.13
		S3.14
		S3.15
		S3.17
		S3.20
	AWS::S3::MultiRegionAccessPoint	S3.24

Servicio de AWS	Tipos de recurso	Controles relacionados
Amazon SageMaker AI	AWS::SageMaker::AppImageConfig	SageMaker6.
	AWS::SageMaker::Image	SageMaker.7.
	AWS::SageMaker::Model	SageMaker5.
	AWS::SageMaker::NotebookInstance	SageMaker2. SageMaker3.
AWS Secrets Manager	AWS::SecretsManager::Secret	SecretsManager1. SecretsManager2. SecretsManager5.
AWS Service Catalog	AWS::ServiceCatalog::Portfolio	ServiceCatalog1.
Amazon Simple Email Service (Amazon SES)	AWS::SES::ConfigurationSet	SES.2
	AWS::SES::ContactList	SES.1
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic	SNS.1
		SNS.3
		SNS.4

Servicio de AWS	Tipos de recurso	Controles relacionados
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue	SQS.1 SQS.2 SQS.3
AWS Step Functions	AWS::Step Functions::StateMachine	StepFunctions1.
	AWS::Step Functions::Activity	StepFunctions2.
AWS Systems Manager (SSM)	AWS::SSM::Document	SSM.5
AWS Transfer Family	AWS::Transfer::Agreement	Transferencia 4.
	AWS::Transfer::Certificate	Transferencia.5
	AWS::Transfer::Connector	Transferencia.3 Transferencia.6
	AWS::Transfer::Profile	Transferencia.7
	AWS::Transfer::Workflow	Transfer.1
AWS WAF	AWS::WAF::Rule	WAF.6

Servicio de AWS	Tipos de recurso	Controles relacionados
	AWS::WAF::RuleGroup	WAF.7
	AWS::WAF::WebACL	WAF.1 WAF.8
	AWS::WAFRegional::Rule	WAF.2
	AWS::WAFRegional::RuleGroup	WAF.3
	AWS::WAFRegional::WebACL	WAF.4
	AWS::WAFv2::RuleGroup	WAF.12
	AWS::WAFv2::WebACL	WAF.10 WAF.11
Amazon WorkSpaces	AWS::WorkSpaces::Workspace	WorkSpaces1. WorkSpaces2.

Recursos necesarios para el estándar AWS fundamental de mejores prácticas de seguridad

Para que Security Hub CSPM informe con precisión las conclusiones de los cambios, los controles activados que se aplican al estándar AWS Foundational Security Best Practices (v.1.0.0), están habilitados y utilizan una AWS Config regla, debe registrar los siguientes tipos de recursos. AWS Config Para obtener información sobre este estándar, consulte. [AWS Estándar fundamental de mejores prácticas de seguridad en Security Hub \(CSPM\)](#)

Servicio de AWS	Tipos de recurso
Amazon API Gateway	<code>AWS::ApiGateway::Stage</code> , <code>AWS::ApiGatewayV2::Stage</code>
AWS AppSync	<code>AWS::AppSync::ApiCache</code> , <code>AWS::AppSync::GraphQLApi</code>
AWS Backup	<code>AWS::Backup::RecoveryPoint</code>
AWS Certificate Manager (ACM)	<code>AWS::ACM::Certificate</code>
AWS CloudFormation	<code>AWS::CloudFormation::Stack</code>
Amazon CloudFront	<code>AWS::CloudFront::Distribution</code>
AWS CodeBuild	<code>AWS::CodeBuild::Project</code> , <code>AWS::CodeBuild::ReportGroup</code>
Amazon Cognito	<code>AWS::Cognito::UserPool</code>
Amazon Connect	<code>AWS::Connect::Instance</code>
AWS DataSync	<code>AWS::DataSync::Task</code>
AWS Database Migration Service (AWS DMS)	<code>AWS::DMS::Endpoint</code> , <code>AWS::DMS::ReplicationInstance</code> , <code>AWS::DMS::ReplicationTask</code>
Amazon DynamoDB	<code>AWS::DynamoDB::Table</code>
Amazon EC2 Systems Manager (SSM)	<code>AWS::SSM::AssociationCompliance</code> , <code>AWS::SSM::ManagedInstanceInventory</code> , <code>AWS::SSM::PatchCompliance</code>
Amazon Elastic Compute Cloud (Amazon EC2)	<code>AWS::EC2::ClientVpnEndpoint</code> , <code>AWS::EC2::Instance</code> , <code>AWS::EC2::LaunchTemplate</code> , <code>AWS::EC2::NetworkAcl</code> , <code>AWS::EC2::NetworkI</code>

Servicio de AWS	Tipos de recurso
	Interface , AWS::EC2::SecurityGroup , AWS::EC2::SpotFleet , AWS::EC2::Subnet , AWS::EC2::TransitGateway , AWS::EC2::VPCElasticNetworkOptions , AWS::EC2::VPNConnection , AWS::EC2::Volume
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup , AWS::AutoScaling::LaunchConfiguration
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::Repository
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS::Cluster , AWS::ECS::Service , AWS::ECS::TaskDefinition , AWS::ECS::TaskSet
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint , AWS::EFS::FileSystem
Amazon Elastic Kubernetes Service (Amazon EKS)	AWS::EKS::Cluster
AWS Elastic Beanstalk	AWS::ElasticBeanstalk::Environment
Elastic Load Balancing	AWS::ElasticLoadBalancing::LoadBalancer , AWS::ElasticLoadBalancingV2::Listener , AWS::ElasticLoadBalancingV2::LoadBalancer
ElasticSearch	AWS::Elasticsearch::Domain
Amazon EMR	AWS::EMR::SecurityConfiguration

Servicio de AWS	Tipos de recurso
AWS Glue	AWS::Glue::Job , AWS::Glue::MLTransform
AWS Identity and Access Management (IAM)	AWS::IAM::Group , AWS::IAM::Policy , AWS::IAM::Role , AWS::IAM::User
Amazon Kinesis	AWS::Kinesis::Stream
AWS Key Management Service (AWS KMS)	AWS::KMS::Key
AWS Lambda	AWS::Lambda::Function
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	AWS::MSK::Cluster , AWS::KafkaConnect::Connector
AWS Network Firewall	AWS::NetworkFirewall::Firewall , AWS::NetworkFirewall::FirewallPolicy , AWS::NetworkFirewall::RuleGroup
OpenSearch Servicio Amazon	AWS::OpenSearch::Domain
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster , AWS::RDS::DBClusterSnapshot , AWS::RDS::DBInstance , AWS::RDS::DBProxy , AWS::RDS::DBSnapshot , AWS::RDS::EventSubscription
Amazon Redshift	AWS::Redshift::Cluster , AWS::Redshift::ClusterSubnetGroup
Amazon Redshift sin servidor	AWS::RedshiftServerless::Workgroup
Amazon Route 53	AWS::Route53::HostedZone

Servicio de AWS	Tipos de recurso
Amazon Simple Storage Service (Amazon S3)	<code>AWS::S3::AccessPoint</code> , <code>AWS::S3::AccountPublicAccessBlock</code> , <code>AWS::S3::Bucket</code> , <code>AWS::S3::MultiRegionAccessPoint</code>
Amazon SageMaker AI	<code>AWS::SageMaker::Model</code> , <code>AWS::SageMaker::NotebookInstance</code>
Amazon Simple Notification Service (Amazon SNS)	<code>AWS::SNS::Topic</code>
Amazon Simple Queue Service (Amazon SQS)	<code>AWS::SQS::Queue</code>
AWS Secrets Manager	<code>AWS::SecretsManager::Secret</code>
AWS Step Functions	<code>AWS::StepFunctions::StateMachine</code>
AWS Transfer Family	<code>AWS::Transfer::Connector</code>
AWS WAF	<code>AWS::WAF::Rule</code> , <code>AWS::WAF::RuleGroup</code> , <code>AWS::WAF::WebACL</code> , <code>AWS::WAFR egional::Rule</code> , <code>AWS::WAFRegional::RuleGroup</code> , <code>AWS::WAFRegional::WebACL</code> , <code>AWS::WAFv2::RuleGroup</code> , <code>AWS::WAFv2::WebACL</code>
Amazon WorkSpaces	<code>AWS::WorkSpaces::Workspace</code>

Recursos necesarios para el índice de referencia de las AWS fundaciones de la CEI

Para ejecutar comprobaciones de seguridad para los controles habilitados que se aplican al Center for Internet Security (CIS) AWS Foundations Benchmark, Security Hub CSPM sigue los pasos de auditoría exactos prescritos para las comprobaciones o utiliza reglas AWS Config gestionadas específicas. Para obtener información sobre este estándar en Security Hub CSPM, consulte. [CIS AWS Foundations es el punto de referencia en Security Hub \(CSPM\)](#)

Recursos necesarios para CIS v3.0.0

Para que Security Hub CSPM informe con precisión de las conclusiones de los controles activados por cambios de CIS v3.0.0 habilitados que utilizan una AWS Config regla, debe registrar los siguientes tipos de recursos en AWS Config

Servicio de AWS	Tipos de recurso
Amazon Elastic Compute Cloud (Amazon EC2)	<code>AWS::EC2::Instance</code> , <code>AWS::EC2::NetworkAcl</code> , <code>AWS::EC2::SecurityGroup</code>
AWS Identity and Access Management (IAM)	<code>AWS::IAM::Group</code> , <code>AWS::IAM::User</code> , <code>AWS::IAM::Role</code>
Amazon Relational Database Service (Amazon RDS)	<code>AWS::RDS::DBInstance</code>
Amazon Simple Storage Service (Amazon S3)	<code>AWS::S3::Bucket</code>

Recursos de necesarios para CIS v1.4.0

Para que Security Hub CSPM informe con precisión de las conclusiones de los controles activados por cambios de CIS v1.4.0 habilitados que utilizan una AWS Config regla, debe registrar los siguientes tipos de recursos en AWS Config

Servicio de AWS	Tipos de recurso
Amazon Elastic Compute Cloud (Amazon EC2)	<code>AWS::EC2::NetworkAcl</code> , <code>AWS::EC2::SecurityGroup</code>
AWS Identity and Access Management (IAM)	<code>AWS::IAM::Policy</code> , <code>AWS::IAM::User</code>
Amazon Relational Database Service (Amazon RDS)	<code>AWS::RDS::DBInstance</code>
Amazon Simple Storage Service (Amazon S3)	<code>AWS::S3::Bucket</code>

Recursos de necesarios para CIS v1.2.0

Para que Security Hub CSPM informe con precisión de las conclusiones de los controles activados por cambios de CIS v1.2.0 habilitados que utilizan una AWS Config regla, debe registrar los siguientes tipos de recursos en. AWS Config

Servicio de AWS	Tipos de recurso
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::SecurityGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Policy , AWS::IAM::User

Recursos necesarios para la norma NIST SP 800-53, revisión 5

Para que Security Hub CSPM informe con precisión las conclusiones de los cambios, los controles activados que se aplican al estándar NIST SP 800-53 revisión 5, están habilitados y utilizan una AWS Config regla, debe registrar los siguientes tipos de recursos. AWS Config Para obtener información sobre este estándar, consulte. [NIST SP 800-53 revisión 5 en Security Hub CSPM](#)

Servicio de AWS	Tipos de recurso
Amazon API Gateway	AWS::ApiGateway::Stage , AWS::ApiGatewayV2::Stage
AWS AppSync	AWS::AppSync::GraphQLApi
AWS Backup	AWS::Backup::RecoveryPoint
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS CloudFormation	AWS::CloudFormation::Stack
Amazon CloudFront	AWS::CloudFront::Distribution
Amazon CloudWatch	AWS::CloudWatch::Alarm
AWS CodeBuild	AWS::CodeBuild::Project

Servicio de AWS	Tipos de recurso
AWS Database Migration Service (AWS DMS)	<code>AWS::DMS::Endpoint</code> , <code>AWS::DMS::ReplicationInstance</code> , <code>AWS::DMS::ReplicationTask</code>
Amazon DynamoDB	<code>AWS::DynamoDB::Table</code>
Amazon Elastic Compute Cloud (Amazon EC2)	<code>AWS::EC2::ClientVpnEndpoint</code> , <code>AWS::EC2::EIP</code> , <code>AWS::EC2::Instance</code> , <code>AWS::EC2::LaunchTemplate</code> , <code>AWS::EC2::NetworkAcl</code> , <code>AWS::EC2::NetworkInterface</code> , <code>AWS::EC2::SecurityGroup</code> , <code>AWS::EC2::Subnet</code> , <code>AWS::EC2::TransitGateway</code> , <code>AWS::EC2::VPNConnection</code> , <code>AWS::EC2::Volume</code>
Amazon EC2 Auto Scaling	<code>AWS::AutoScaling::AutoScalingGroup</code> , <code>AWS::AutoScaling::LaunchConfiguration</code>
Amazon Elastic Container Registry (Amazon ECR)	<code>AWS::ECR::Repository</code>
Amazon Elastic Container Service (Amazon ECS)	<code>AWS::ECS::Cluster</code> , <code>AWS::ECS::Service</code> , <code>AWS::ECS::TaskDefinition</code>
Amazon Elastic File System (Amazon EFS)	<code>AWS::EFS::AccessPoint</code>
Amazon Elastic Kubernetes Service (Amazon EKS)	<code>AWS::EKS::Cluster</code>
AWS Elastic Beanstalk	<code>AWS::ElasticBeanstalk::Environment</code>

Servicio de AWS	Tipos de recurso
Elastic Load Balancing	<code>AWS::ElasticLoadBalancing::LoadBalancer</code> , <code>AWS::ElasticLoadBalancingV2::Listener</code> , <code>AWS::ElasticLoadBalancingV2::LoadBalancer</code>
Amazon ElasticSearch	<code>AWS::Elasticsearch::Domain</code>
Amazon EMR	<code>AWS::EMR::SecurityConfiguration</code>
Amazon EventBridge	<code>AWS::Events::Endpoint</code> , <code>AWS::Events::EventBus</code>
AWS Glue	<code>AWS::Glue::Job</code>
AWS Identity and Access Management (IAM)	<code>AWS::IAM::Group</code> , <code>AWS::IAM::Policy</code> , <code>AWS::IAM::Role</code> , <code>AWS::IAM::User</code>
AWS Key Management Service (AWS KMS)	<code>AWS::KMS::Alias</code> , <code>AWS::KMS::Key</code>
Amazon Kinesis	<code>AWS::Kinesis::Stream</code>
AWS Lambda	<code>AWS::Lambda::Function</code>
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	<code>AWS::MSK::Cluster</code>
Amazon MQ	<code>AWS::AmazonMQ::Broker</code>
AWS Network Firewall	<code>AWS::NetworkFirewall::Firewall</code> , <code>AWS::NetworkFirewall::FirewallPolicy</code> , <code>AWS::NetworkFirewall::RuleGroup</code>
OpenSearch Servicio Amazon	<code>AWS::OpenSearch::Domain</code>

Servicio de AWS	Tipos de recurso
Amazon Relational Database Service (Amazon RDS)	<code>AWS::RDS::DBCluster</code> , <code>AWS::RDS::DBClusterSnapshot</code> , <code>AWS::RDS::DBInstance</code> , <code>AWS::RDS::DBSnapshot</code> , <code>AWS::RDS::EventSubscription</code>
Amazon Redshift	<code>AWS::Redshift::Cluster</code> , <code>AWS::Redshift::ClusterSubnetGroup</code>
Amazon Route 53	<code>AWS::Route53::HostedZone</code>
Amazon Simple Storage Service (Amazon S3)	<code>AWS::S3::AccessPoint</code> , <code>AWS::S3::AccountPublicAccessBlock</code> , <code>AWS::S3::Bucket</code>
AWS Service Catalog	<code>AWS::ServiceCatalog::Portfolio</code>
Amazon Simple Notification Service (Amazon SNS)	<code>AWS::SNS::Topic</code>
Amazon Simple Queue Service (Amazon SQS)	<code>AWS::SQS::Queue</code>
Amazon EC2 Systems Manager (SSM)	<code>AWS::SSM::AssociationCompliance</code> , <code>AWS::SSM::ManagedInstanceInventory</code> , <code>AWS::SSM::PatchCompliance</code>
Amazon SageMaker AI	<code>AWS::SageMaker::NotebookInstance</code>
AWS Secrets Manager	<code>AWS::SecretsManager::Secret</code>
AWS Transfer Family	<code>AWS::Transfer::Connector</code>

Servicio de AWS	Tipos de recurso
AWS WAF	AWS::WAF::Rule , AWS::WAF::RuleGroup , AWS::WAF::WebACL , AWS::WAFRegional::Rule , AWS::WAFRegional::RuleGroup , AWS::WAFRegional::WebACL , AWS::WAFv2::RuleGroup , AWS::WAFv2::WebACL

Recursos necesarios para la norma NIST SP 800-171, revisión 2

Para que Security Hub CSPM informe con precisión las conclusiones de los cambios, los controles activados que se aplican al estándar NIST SP 800-171 revisión 2, están habilitados y utilizan una AWS Config regla, debe registrar los siguientes tipos de recursos. AWS Config Para obtener información sobre este estándar, consulte. [NIST SP 800-171 revisión 2 en Security Hub CSPM](#)

Servicio de AWS	Tipos de recurso
AWS Certificate Manager(ACM)	AWS::ACM::Certificate
Amazon API Gateway	AWS::ApiGateway::Stage
Amazon CloudFront	AWS::CloudFront::Distribution
Amazon CloudWatch	AWS::CloudWatch::Alarm
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::ClientVpnEndpoint , AWS::EC2::NetworkAcl , AWS::EC2::SecurityGroup , AWS::EC2::VPC , AWS::EC2::VPNConnection
Elastic Load Balancing	AWS::ElasticLoadBalancing::LoadBalancer
AWS Identity and Access Management(IAM)	AWS::IAM::Policy , AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias , AWS::KMS::Key

Servicio de AWS	Tipos de recurso
AWS Network Firewall	AWS::NetworkFirewall::FirewallPolicy , AWS::NetworkFirewall::RuleGroup
Amazon Simple Storage Service (Amazon S3)	AWS::S3::Bucket
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic
AWS Systems Manager(SSM)	AWS::SSM::PatchCompliance
AWS WAF	AWS::WAFv2::RuleGroup

Recursos necesarios para PCI DSS v3.2.1

Para que Security Hub CSPM informe con precisión las conclusiones de los controles que se aplican a la versión 3.2.1 del Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS), están habilitados y utilizan una AWS Config regla, debe registrar los siguientes tipos de recursos. AWS Config Para obtener información sobre este estándar, consulte. [PCI DSS en Security Hub CSPM](#)

Servicio de AWS	Tipos de recurso
AWS CodeBuild	AWS::CodeBuild::Project
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::EIP , AWS::EC2::Instance , AWS::EC2::SecurityGroup
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Policy , AWS::IAM::User
AWS Lambda	AWS::Lambda::Function
OpenSearch Servicio Amazon	AWS::OpenSearch::Domain

Servicio de AWS	Tipos de recurso
Amazon Relational Database Service (Amazon RDS)	<code>AWS::RDS::DBClusterSnapshot</code> , <code>AWS::RDS::DBInstance</code> , <code>AWS::RDS::DBSnapshot</code>
Amazon Redshift	<code>AWS::Redshift::Cluster</code>
Amazon Simple Storage Service (Amazon S3)	<code>AWS::S3::AccountPublicAccessBlock</code> , <code>AWS::S3::Bucket</code>
Amazon EC2 Systems Manager (SSM)	<code>AWS::SSM::AssociationCompliance</code> , <code>AWS::SSM::ManagedInstanceInventory</code> , <code>AWS::SSM::PatchCompliance</code>

Recursos necesarios para el estándar de etiquetado AWS de recursos

Todos los controles que se aplican al estándar de etiquetado de AWS recursos se activan mediante cambios y utilizan una AWS Config regla. Para que Security Hub CSPM informe con precisión de los hallazgos de estos controles, debe registrar los siguientes tipos de recursos en AWS Config. Para obtener información sobre este estándar, consulte [AWS Estándar de etiquetado de recursos en Security Hub \(CSPM\)](#).

Servicio de AWS	Tipos de recurso
AWS Amplify	<code>AWS::Amplify::App</code> , <code>AWS::Amplify::Branch</code>
Amazon AppFlow	<code>AWS::AppFlow::Flow</code>
AWS App Runner	<code>AWS::AppRunner::Service</code> , <code>AWS::AppRunner::VpcConnector</code>
AWS AppConfig	<code>AWS::AppConfig::Application</code> , <code>AWS::AppConfig::ConfigurationProfile</code> , <code>AWS::AppConfig::Environment</code>

Servicio de AWS	Tipos de recurso
	<code>Environment</code> , <code>AWS::AppConfig::ExtensionAssociation</code>
AWS AppSync	<code>AWS::AppSync::GraphQLApi</code>
Amazon Athena	<code>AWS::Athena::DataCatalog</code> , <code>AWS::Athena::WorkGroup</code>
AWS Backup	<code>AWS::Backup::BackupPlan</code> , <code>AWS::Backup::BackupVault</code> , <code>AWS::Backup::RecoveryPlan</code> , <code>AWS::Backup::ReportPlan</code>
AWS Batch	<code>AWS::Batch::ComputeEnvironment</code> , <code>AWS::Batch::JobQueue</code> , <code>AWS::Batch::SchedulingPolicy</code>
AWS Certificate Manager (ACM)	<code>AWS::ACM::Certificate</code>
AWS CloudFormation	<code>AWS::CloudFormation::Stack</code>
Amazon CloudFront	<code>AWS::CloudFront::Distribution</code>
AWS CloudTrail	<code>AWS::CloudTrail::Trail</code>
AWS CodeArtifact	<code>AWS::CodeArtifact::Repository</code>
Amazon CodeGuru	<code>AWS::CodeGuruProfiler::ProfilingGroup</code> , <code>AWS::CodeGuruReviewer::RepositoryAssociation</code>
Amazon Connect	<code>AWS::CustomerProfiles::ObjectType</code>

Servicio de AWS	Tipos de recurso
AWS Database Migration Service (AWS DMS)	AWS::DMS::Certificate , AWS::DMS::EventSubscription AWS::DMS::ReplicationInstance , AWS::DMS::ReplicationSubnetGroup
AWS DataSync	AWS::DataSync::Task
Amazon Detective	AWS::Detective::Graph
Amazon DynamoDB	AWS::DynamoDB::Trail
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::CustomerGateway , AWS::EC2::DHCPOptions , AWS::EC2::EIP , AWS::EC2::FlowLog , AWS::EC2::Instance , AWS::EC2::InternetGateway , AWS::EC2::LaunchTemplate , AWS::EC2::NatGateway , AWS::EC2::NetworkAcl , AWS::EC2::NetworkInterface , AWS::EC2::PrefixList , AWS::EC2::RouteTable , AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::TrafficMirrorFilter , AWS::EC2::TrafficMirrorSession , AWS::EC2::TrafficMirrorTarget , AWS::EC2::TransitGateway , AWS::EC2::TransitGatewayAttachment , AWS::EC2::TransitGatewayRouteTable , AWS::EC2::Volume , AWS::EC2::VPC , AWS::EC2::VPCEndpointService , AWS::EC2::VPCPeeringConnection , AWS::EC2::VPNGateway

Servicio de AWS	Tipos de recurso
Amazon EC2 Auto Scaling	<code>AWS::AutoScaling::AutoScalingGroup</code>
Amazon Elastic Container Registry (Amazon ECR)	<code>AWS::ECR::PublicRepository</code>
Amazon Elastic Container Service (Amazon ECS)	<code>AWS::ECS::Cluster</code> , <code>AWS::ECS::Service</code> , <code>AWS::ECS::TaskDefinition</code>
Amazon Elastic File System (Amazon EFS)	<code>AWS::EFS::AccessPoint</code>
Amazon Elastic Kubernetes Service (Amazon EKS)	<code>AWS::EKS::Cluster</code> , <code>AWS::EKS::IdentityProviderConfig</code>
AWS Elastic Beanstalk	<code>AWS::ElasticBeanstalk::Environment</code>
ElasticSearch	<code>AWS::Elasticsearch::Domain</code>
Amazon EventBridge	<code>AWS::Events::EventBus</code>
Amazon Fraud Detector	<code>AWS::FraudDetector::EntityType</code> , <code>AWS::FraudDetector::Label</code> <code>AWS::FraudDetector::Outcome</code> , <code>AWS::FraudDetector::Variable</code>
AWS Global Accelerator	<code>AWS::GlobalAccelerator::Accelerator</code>
AWS Glue	<code>AWS::Glue::Job</code>
Amazon GuardDuty	<code>AWS::GuardDuty::Detector</code> , <code>AWS::GuardDuty::Filter</code> , <code>AWS::GuardDuty::IPSet</code>
AWS Identity and Access Management (IAM)	<code>AWS::IAM::Role</code> , <code>AWS::IAM::User</code>

Servicio de AWS	Tipos de recurso
AWS Identity and Access Management Access Analyzer (Analizador de acceso IAM)	<code>AWS::AccessAnalyzer::Analyzer</code>
AWS IoT	<code>AWS::IoT::Authorizer</code> , <code>AWS::IoT::Dimension</code> , <code>AWS::IoT::MitigationAction</code> , <code>AWS::IoT::Policy</code> , <code>AWS::IoT::RoleAlias</code> , <code>AWS::IoT::SecurityProfile</code>
AWS IoT Eventos	<code>AWS::IoTEvents::AlarmModel</code> , <code>AWS::IoTEvents::DetectorModel</code> , <code>AWS::IoTEvents::Input</code>
AWS IoT SiteWise	<code>AWS::IoTSiteWise::Dashboard</code> , <code>AWS::IoTSiteWise::Gateway</code> , <code>AWS::IoTSiteWise::Portal</code> , <code>AWS::IoTSiteWise::Project</code>
AWS IoT TwinMaker	<code>AWS::IoTTwinMaker::Entity</code> , <code>AWS::IoTTwinMaker::Scene</code> , <code>AWS::IoTTwinMaker::SyncJob</code> , <code>AWS::IoTTwinMaker::Workspace</code>
AWS IoT inalámbrico	<code>AWS::IoTWireless::FuotaTask</code> , <code>AWS::IoTWireless::MulticastGroup</code> , <code>AWS::IoTWireless::ServiceProfile</code>
Amazon Interactive Video Service (Amazon IVS)	<code>AWS::IVS::Channel</code> , <code>AWS::IVS::PlaybackKeyPair</code> , <code>AWS::IVS::RecordingConfiguration</code>
Amazon Keyspaces (para Apache Cassandra)	<code>AWS::Cassandra::Keyspace</code>
Amazon Kinesis	<code>AWS::Kinesis::Stream</code>
AWS Lambda	<code>AWS::Lambda::Function</code>

Servicio de AWS	Tipos de recurso
Amazon MQ	AWS::AmazonMQ::Broker
AWS Network Firewall	AWS::NetworkFirewall::Firewall , AWS::NetworkFirewall::FirewallPolicy
OpenSearch Servicio Amazon	AWS::OpenSearch::Domain
AWS Private Certificate Authority	AWS::ACMPCA::CertificateAuthority
Amazon Relational Database Service	AWS::RDS::DBCluster , AWS::RDS::DBClusterSnapshot , AWS::RDS::DBInstance , AWS::RDS::DBSecurityGroup , AWS::RDS::DBSnapshot , AWS::RDS::DBSubnetGroup
Amazon Redshift	AWS::Redshift::Cluster , AWS::Redshift::ClusterParameterGroup , AWS::Redshift::ClusterSnapshot , AWS::Redshift::ClusterSubnetGroup , AWS::Redshift::EventSubscription
Amazon Route 53	AWS::Route53::HealthCheck
Amazon SageMaker AI	AWS::SageMaker::AppImageConfig , AWS::SageMaker::Image
AWS Secrets Manager	AWS::SecretsManager::Secret
Amazon Simple Email Service (Amazon SES)	AWS::SES::ConfigurationSet , AWS::SES::ContactList
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic

Servicio de AWS	Tipos de recurso
Amazon Simple Queue Service (Amazon SQS)	<code>AWS::SQS::Queue</code>
AWS Step Functions	<code>AWS::StepFunctions::Activity</code>
AWS Systems Manager (SSM)	<code>AWS::SSM::Document</code>
AWS Transfer Family	<code>AWS::Transfer::Agreement</code> , <code>AWS::Transfer::Certificate</code> , <code>AWS::Transfer::Connector</code> , <code>AWS::Transfer::Profile</code> , <code>AWS::Transfer::Workflow</code>

Recursos necesarios para el estándar de gestión de AWS Control Tower servicios

Para que el CSPM de Security Hub informe con precisión de los resultados de los controles activados por cambios que se aplican al estándar de AWS Control Tower gestión de servicios, están habilitados y utilizan una AWS Config regla, debe registrar los siguientes tipos de recursos. AWS Config Para obtener información sobre este estándar, consulte. [Estándar gestionado por el servicio: AWS Control Tower](#)

Servicio de AWS	Tipos de recurso
Amazon API Gateway	<code>AWS::ApiGateway::Stage</code> <code>AWS::ApiGatewayV2::Stage</code>
AWS Certificate Manager (ACM)	<code>AWS::ACM::Certificate</code>
AWS CodeBuild	<code>AWS::CodeBuild::Project</code>
Amazon DynamoDB	<code>AWS::DynamoDB::Table</code>
Amazon Elastic Compute Cloud (EC2)	<code>AWS::EC2::Instance</code> <code>AWS::EC2::NetworkAcl</code> <code>AWS::EC2::NetworkInterface</code>

Servicio de AWS	Tipos de recurso
	AWS::EC2::SecurityGroup AWS::EC2::Subnet AWS::EC2::VPNConnection AWS::EC2::Volume
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup AWS::AutoScaling::LaunchConfiguration
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::Repository
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS::Cluster AWS::ECS::Service AWS::ECS::TaskDefinition
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint
Amazon EKS	AWS::EKS::Cluster
ElasticBeanstalk	AWS::ElasticBeanstalk::Environment
Elastic Load Balancing	AWS::ElasticLoadBalancing::LoadBalancer AWS::ElasticLoadBalancingV2::LoadBalancer
ElasticSearch	AWS::Elasticsearch::Domain

Servicio de AWS	Tipos de recurso
AWS Identity and Access Management (IAM)	AWS::IAM::Group AWS::IAM::Policy AWS::IAM::Role AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias AWS::KMS::Key
Amazon Kinesis	AWS::Kinesis::Stream
AWS Lambda	AWS::Lambda::Function
AWS Network Firewall	AWS::NetworkFirewall::FirewallPolicy AWS::NetworkFirewall::RuleGroup
OpenSearch Servicio Amazon	AWS::OpenSearch::Domain
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster AWS::RDS::DBClusterSnapshot AWS::RDS::DBInstance AWS::RDS::DBSnapshot AWS::RDS::EventSubscription
Amazon Redshift	AWS::Redshift::Cluster
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccountPublicAccessBlock AWS::S3::Bucket

Servicio de AWS	Tipos de recurso
Amazon Simple Notification Service (Amazon SNS)	<code>AWS::SNS::Topic</code>
Amazon Simple Queue Service (Amazon SQS)	<code>AWS::SQS::Queue</code>
AWS Secrets Manager	<code>AWS::SecretsManager::Secret</code>
Amazon EC2 Systems Manager (SSM)	<code>AWS::SSM::AssociationCompliance</code> <code>AWS::SSM::ManagedInstanceInventory</code> <code>AWS::SSM::PatchCompliance</code>
AWS WAF	<code>AWS::WAFRegional::Rule</code> <code>AWS::WAFRegional::RuleGroup</code> <code>AWS::WAFRegional::WebACL</code> <code>AWS::WAFv2::WebACL</code>

Programación para ejecutar comprobaciones de seguridad

Tras activar un estándar de seguridad, Security Hub Cloud AWS Security Posture Management (CSPM) comienza a ejecutar todas las comprobaciones en un plazo de dos horas. La mayoría de las comprobaciones comienzan a ejecutarse en 25 minutos. Security Hub CSPM ejecuta las comprobaciones evaluando la regla subyacente a un control. Hasta que un control complete su primera ejecución de comprobaciones, su estado es Sin datos.

Al habilitar un nuevo estándar, Security Hub CSPM puede tardar hasta 24 horas en generar resultados para los controles que utilizan la misma regla subyacente AWS Config vinculada a servicios que los controles habilitados de otros estándares habilitados. Por ejemplo, si habilita el control [Lambda.1](#) en el estándar AWS Foundational Security Best Practices (FSBP), Security Hub CSPM crea la regla vinculada al servicio y, por lo general, genera resultados en cuestión de minutos. Después de esto, si habilita el control Lambda.1 en el Estándar de seguridad de datos de la

industria de tarjetas de pago (PCI DSS), Security Hub CSPM puede tardar hasta 24 horas en generar resultados para el control, ya que utiliza la misma regla vinculada al servicio.

Después de la comprobación inicial, la programación de cada control puede ser periódica o activada por cambios. En el caso de un control que se basa en una AWS Config regla gestionada, la descripción del control incluye un enlace a la descripción de la regla en la Guía para desarrolladores.AWS Config En esa descripción se especifica si la regla se desencadena por cambios o es periódica.

Controles de seguridad periódicos

Los controles de seguridad periódicos se ejecutan automáticamente en las 12 o 24 horas posteriores a la última ejecución. Security Hub CSPM determina la periodicidad y no se puede cambiar. Los controles periódicos reflejan una evaluación en el momento en que se ejecuta la comprobación.

Si actualiza el estado de flujo de trabajo de un resultado de control periódico y, a continuación, en la siguiente comprobación, el estado de cumplimiento del resultado sigue siendo el mismo, el estado de flujo de trabajo permanece en su estado modificado. Por ejemplo, si encuentra un error en la búsqueda del control [KMS.4](#) (la AWS KMS key rotación debe estar habilitada) y, a continuación, corrige la búsqueda, Security Hub CSPM cambia el estado del flujo de trabajo de a. NEW RESOLVED Si desactiva la rotación de claves de KMS antes de la siguiente comprobación periódica, el estado del flujo de trabajo del resultado se mantiene como RESOLVED.

Las comprobaciones que utilizan funciones Lambda personalizadas de CSPM de Security Hub son periódicas.

Controles de seguridad desencadenados por cambios

Las comprobaciones de seguridad activadas por cambios se ejecutan cuando el recurso asociado cambia de estado. AWS Config le permite elegir entre el registro continuo de los cambios en el estado del recurso y el registro diario. Si elige el registro diario, AWS Config entrega los datos de configuración de los recursos al final de cada período de 24 horas si se producen cambios en el estado de los recursos. Si no hay cambios, no se entrega ningún dato. Esto puede retrasar la generación de las conclusiones del CSPM de Security Hub hasta que se complete un período de 24 horas. Independientemente del período de grabación que haya elegido, el CSPM de Security Hub comprueba cada 18 horas para asegurarse de que no AWS Config se haya perdido ninguna actualización de recursos.

En general, Security Hub CSPM utiliza reglas activadas por cambios siempre que es posible. Para que un recurso utilice una regla activada por cambios, debe admitir los elementos de configuración. AWS Config

Generación y actualización de los resultados de control

AWS Security Hub Cloud Security Posture Management (CSPM) genera resultados de control cuando comprueba los controles de seguridad. Los resultados de control utilizan el [formato AWS de búsqueda de seguridad \(ASFF\)](#).

Security Hub CSPM normalmente cobra por cada control de seguridad de un control. Sin embargo, si varios controles utilizan la misma AWS Config regla, Security Hub CSPM solo cobrará una vez por cada comprobación que se ajuste a la regla. Por ejemplo, varios controles utilizan la AWS Config `iam-password-policy` regla en el estándar CIS AWS Foundations Benchmark y en el estándar AWS Foundational Security Best Practices. Cada vez que Security Hub CSPM realiza una comprobación según esa regla, genera una comprobación de control independiente para cada control relacionado, pero solo cobra una vez por la comprobación.

Si el tamaño de un hallazgo de control supera el máximo de 240 KB, Security Hub CSPM elimina el `Resource.Details` objeto del hallazgo. En el caso de los controles respaldados por AWS Config recursos, puede revisar los detalles de los recursos mediante la AWS Config consola.

Temas

- [Resultados de control consolidados](#)
- [Generar, actualizar y archivar las conclusiones de control](#)
- [Automatización y supresión de los resultados de control](#)
- [Detalles de conformidad de los resultados del control](#)
- [ProductFields detalles de los hallazgos de control](#)
- [Niveles de gravedad de los hallazgos de control](#)

Resultados de control consolidados

Si los hallazgos de control consolidados están habilitados para su cuenta, Security Hub CSPM genera un único hallazgo nuevo o una actualización de hallazgos para cada comprobación de seguridad de un control, incluso si un control se aplica a varios estándares habilitados. Para obtener una lista de los controles y los estándares a los que se aplican, consulte la [Referencia de control](#)

[para Security Hub CSPM](#) Recomendamos habilitar los resultados de control consolidados para reducir el ruido de resultados.

Si habilitó el CSPM de Security Hub Cuenta de AWS antes del 23 de febrero de 2023, puede habilitar los hallazgos de control consolidados siguiendo las instrucciones que aparecen más adelante en esta sección. Si habilitas el CSPM de Security Hub a partir del 23 de febrero de 2023, los hallazgos de control consolidados se habilitarán automáticamente para tu cuenta.

Si utiliza la [integración CSPM de Security Hub con](#) las cuentas de los miembros AWS Organizations o las invita mediante un [proceso de invitación manual](#), las conclusiones de control consolidadas solo se habilitan para las cuentas de los miembros si están habilitadas para la cuenta de administrador. Si la función está deshabilitada para la cuenta de administrador, estará deshabilitada para las cuentas de los miembros. Este comportamiento se aplica a las cuentas de miembros nuevas y existentes. Además, si el administrador usa la [configuración central](#) para administrar el CSPM de Security Hub para varias cuentas, no podrá usar políticas de configuración central para habilitar o deshabilitar los hallazgos de control consolidados para las cuentas.

Si deshabilita las conclusiones de control consolidadas para su cuenta, Security Hub CSPM genera una conclusión de control independiente para cada comprobación de seguridad y cada estándar habilitado que incluya un control. Por ejemplo, si habilita cuatro estándares que comparten un control, recibirá cuatro conclusiones distintas tras una comprobación de seguridad del control. Si habilita los resultados de control consolidados, solo recibirá un resultado.

Cuando habilita los hallazgos de control consolidados, Security Hub CSPM crea nuevos hallazgos independientes de los estándares y archiva los hallazgos originales basados en estándares. Algunos valores y campos de búsqueda de controles cambiarán, lo que podría afectar a sus flujos de trabajo actuales. Para obtener información sobre estos cambios, consulte [Resultados de control consolidados: cambios en ASFF](#). La activación de los hallazgos de control consolidados también puede afectar a los hallazgos que los productos integrados de terceros reciben de Security Hub CSPM. Si utiliza la solución [Automated Security Response en la AWS versión 2.0.0](#), tenga en cuenta que respalda los resultados de control consolidados.

Para habilitar o deshabilitar los resultados de control consolidados, debe iniciar sesión en una cuenta de administrador o en una cuenta independiente.

 Note

Una vez habilitadas las conclusiones de control consolidadas, Security Hub CSPM puede tardar hasta 24 horas en generar nuevas conclusiones consolidadas y archivar las

conclusiones originales basadas en estándares. Del mismo modo, después de deshabilitar las conclusiones de control consolidadas, Security Hub CSPM puede tardar hasta 24 horas en generar nuevas conclusiones basadas en estándares y archivar las conclusiones consolidadas. Durante estos períodos, es posible que vea en su cuenta una combinación de hallazgos independientes de los estándares y basados en estándares.

Security Hub CSPM console

Para activar o desactivar las conclusiones de control consolidadas

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, en Configuración, seleccione General.
3. En la sección Controles, selecciona Editar.
4. Utilice el conmutador de conclusiones de control consolidadas para activar o desactivar las conclusiones de control consolidadas.
5. Seleccione Save.

Security Hub CSPM API

Para habilitar o deshabilitar las conclusiones de control consolidadas mediante programación, utilice la API [UpdateSecurityHubConfiguration](#) CSPM de Security Hub. O bien, si está utilizando el AWS CLI, ejecute el comando. [update-security-hub-configuration](#)

Para el control-finding-generator parámetro, especifique si desea SECURITY_CONTROL habilitar los hallazgos de control consolidados. Para deshabilitar los hallazgos de control consolidados, especifique STANDARD_CONTROL.

Por ejemplo, el siguiente AWS CLI comando habilita los hallazgos de control consolidados.

```
$ aws securityhub --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

El siguiente AWS CLI comando desactiva las conclusiones de control consolidadas.

```
$ aws securityhub --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

Generar, actualizar y archivar las conclusiones de control

[Security Hub CSPM ejecuta los controles de seguridad según un cronograma.](#) Una comprobación posterior con respecto a un control determinado puede generar un nuevo resultado. Por ejemplo, el estado de un control podría cambiar de FAILED a PASSED. En este caso, Security Hub CSPM genera un nuevo hallazgo que contiene el resultado más reciente. Si una comprobación posterior con respecto a un control determinado genera un resultado idéntico al resultado actual, Security Hub CSPM actualiza el resultado existente. No se genera un nuevo hallazgo.

Además de generar y actualizar las conclusiones de control, Security Hub CSPM archiva automáticamente las conclusiones de control que cumplen determinados criterios. Security Hub CSPM archiva un hallazgo si el control está deshabilitado, el recurso especificado se elimina o el recurso especificado ya no existe. Es posible que un recurso ya no exista porque el servicio asociado ya no se utiliza. Más específicamente, Security Hub CSPM archiva automáticamente un hallazgo de control si el hallazgo cumple uno de los siguientes criterios:

- El hallazgo no se ha actualizado desde hace entre 3 y 5 días. Tenga en cuenta que el archivado basado en este período de tiempo se hace con el máximo esfuerzo y no está garantizado.
- Se devolvió la AWS Config evaluación asociada NOT_APPLICABLE para determinar el estado de conformidad del recurso especificado.

Para determinar si una constatación está archivada, puede consultar el campo de estado de registro (RecordState) de la constatación. Si se archiva un hallazgo, el valor de este campo es. ARCHIVED

Security Hub CSPM almacena las conclusiones de control archivadas durante 30 días. Transcurridos 30 días, los hallazgos caducan y Security Hub CSPM los elimina permanentemente. Para determinar si una constatación de control archivada ha caducado, Security Hub CSPM basa su cálculo en el valor del UpdatedAt campo de la constatación.

Para almacenar las conclusiones de control archivadas durante más de 30 días, puede exportarlas a un bucket de S3. Puedes hacerlo mediante una acción personalizada con una EventBridge regla de Amazon. Para obtener más información, consulte [Uso EventBridge para respuesta y remediación automatizadas](#).

Automatización y supresión de los resultados de control

Puede usar las reglas de automatización de CSPM de Security Hub para actualizar o suprimir hallazgos de control específicos. Si suprimes un hallazgo, puedes seguir accediendo a él desde tu

cuenta. Sin embargo, la supresión indica que usted cree que no es necesario tomar ninguna medida para abordar la conclusión.

Al suprimir los hallazgos, puede reducir el ruido que genera la detección. Por ejemplo, puede suprimir los resultados de control que se generan en las cuentas de prueba. O bien, puede suprimir los hallazgos relacionados con recursos específicos. Para obtener más información sobre cómo actualizar o suprimir los hallazgos automáticamente, consulte [Descripción de las reglas de automatización en Security Hub CSPM](#).

Las reglas de automatización son adecuadas cuando se desean actualizar o suprimir hallazgos de control específicos. Sin embargo, si un control no es relevante para su organización o caso de uso, le recomendamos que lo [desactive](#). Cuando inhabilitas un control, Security Hub CSPM no realiza controles de seguridad en él y no se te cobra por ello.

Detalles de conformidad de los resultados del control

En los resultados generados por las comprobaciones de seguridad de los controles, el [Compliance](#) objeto y los campos del formato de comprobación de AWS seguridad (ASFF) proporcionan los detalles de conformidad de los recursos individuales comprobados por un control. Esto incluye la siguiente información:

- **AssociatedStandards**— Los estándares habilitados en los que está habilitado el control.
- **RelatedRequirements**— Los requisitos relacionados con el control en todos los estándares habilitados. Estos requisitos se derivan de marcos de seguridad de terceros para el control, como el estándar de seguridad de datos del sector de las tarjetas de pago (PCI DSS) o el estándar NIST SP 800-171, revisión 2.
- **SecurityControlId**— El identificador para el control en todos los estándares compatibles con el Security Hub CSPM.
- **Status**— El resultado de la comprobación más reciente que Security Hub CSPM realizó para el control. Los resultados de las comprobaciones anteriores se guardan archivados.
- **StatusReasons**— Una matriz que enumera los motivos del valor especificado en el Status campo. Para cada motivo, incluye un código de motivo y una descripción.

En la siguiente tabla se enumeran los códigos de motivo y las descripciones que un hallazgo podría incluir en la StatusReasons matriz. Los pasos de corrección varían en función del control que haya generado un hallazgo con un código de motivo específico. Para revisar la guía de corrección de un control, consulte la [Referencia de control para Security Hub CSPM](#)

Código de motivo	Compliance status (Estado de conformidad)	Descripción
CLOUDTRAIL_METRIC_FILTER_NOT_VALID	FAILED	El registro CloudTrail multirregional no tiene un filtro métrico válido.
CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT	FAILED	Los filtros métricos no están presentes en el sendero multirregional. CloudTrail
CLOUDTRAIL_MULTI_REGION_NOT_PRESENT	FAILED	La cuenta no tiene un registro multirregional CloudTrail con la configuración requerida.
CLOUDTRAIL_REGION_INVALID	WARNING	Los CloudTrail senderos multirregionales no se encuentran en la región actual.
CLOUDWATCH_ALARM_ACTIONS_NOT_VALID	FAILED	No hay acciones de alarma válidas presentes.
CLOUDWATCH_ALARMS_NOT_PRESENT	FAILED	CloudWatch las alarmas no existen en la cuenta.
CONFIG_ACCESS_DENIED	NOT_AVAILABLE AWS Config el estado es ConfigError	AWS Config acceso denegado. Compruebe que AWS Config está activado y que se le han concedido los permisos suficientes.
CONFIG_EVALUATIONS_EMPTY	PASSED	AWS Config evaluó sus recursos en función de la regla. La regla no se aplicaba a los AWS recursos incluidos en su ámbito, se eliminaron los recursos especificados

Código de motivo	Compliance status (Estado de conformidad)	Descripción
		o se eliminaron los resultados de la evaluación.
CONFIG_RECORDER_CUSTOM_ROLE	FAILED(para Config.1)	La AWS Config grabadora usa un rol de IAM personalizado en lugar del rol AWS Config vinculado al servicio, y el parámetro <code>includeConfigServiceLinkedRoleCheck</code> personalizado de Config.1 no está establecido en <code>false</code>
CONFIG_RECORDER_DISABLED	FAILED(para Config.1)	AWS Config no está activado con la grabadora de configuración encendida.
CONFIG_RECORDER_MISSING_REQUIRED_RESOURCE_TYPES	FAILED(para Config.1)	AWS Config no registra todos los tipos de recursos que corresponden a los controles CSPM de Security Hub habilitados. Active la grabación de los siguientes recursos: <i>. Resources that aren't being recorded</i>

Código de motivo	Compliance status (Estado de conformidad)	Descripción
CONFIG_RETURNS_NOT_APPLICABLE	NOT_AVAILABLE	El estado de cumplimiento se NOT_AVAILABLE debe a que AWS Config devolvió el estado de No aplicable. AWS Config no indica el motivo del estado. Estas son algunas de las posibles razones del estado de No aplicable: • El recurso se ha eliminado del ámbito de aplicación de la AWS Config regla. • Se ha eliminado la AWS Config regla. • Se ha eliminado el recurso. • La lógica de la AWS Config regla puede generar un estado de No aplicable.

Código de motivo	Compliance status (Estado de conformidad)	Descripción
CONFIG_RULE_EVALUATION_ERROR	NOT_AVAILABLE AWS Config el estado es ConfigError	Este código de motivo se utiliza para varios tipos diferentes de errores de evaluación. La descripción proporciona la información específica del motivo. El tipo de error puede ser uno de los siguientes: • Incapacidad de realizar la evaluación debido a la falta de permisos. La descripción proporciona el permiso específico que falta. • Un valor ausente o no válido para un parámetro. La descripción proporciona el parámetro y los requisitos para el valor del parámetro. • Error al leer en un bucket de S3. La descripción identifica el bucket y proporciona el error específico. • Falta una AWS suscripción. • Un tiempo de espera general en la evaluación. • Una cuenta suspendida.
CONFIG_RULE_NOT_FOUND	NOT_AVAILABLE AWS Config el estado es ConfigError	La AWS Config regla está en proceso de creación.

Código de motivo	Compliance status (Estado de conformidad)	Descripción
INTERNAL_SERVICE_ERROR	NOT_AVAILABLE	Se ha producido un error desconocido.
LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE	FAILED	El CSPM de Security Hub no puede realizar una comprobación con un entorno de ejecución de Lambda personalizado.
S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION	WARNING	El hallazgo se encuentra en un WARNING estado debido a que el depósito de S3 asociado a esta regla se encuentra en una región o cuenta diferente. Esta regla no admite comprobaciones entre regiones ni entre cuentas. Se recomienda deshabilitar este control en esta región o cuenta. Ejecútelo solo en la región o cuenta donde se encuentra el recurso.
SNS_SUBSCRIPTION_NOT_PRESENT	FAILED	Los filtros de métricas de CloudWatch Logs no tienen una suscripción a Amazon SNS válida.

Código de motivo	Compliance status (Estado de conformidad)	Descripción
SNS_TOPIC_CROSS_ACCOUNT	WARNING	El resultado se encuentra en un estado de WARNING. El tema de SNS asociado a esta regla es propiedad de otra cuenta. La cuenta actual no puede obtener la información de la suscripción. La cuenta propietaria del tema de SNS debe conceder a la cuenta actual el permiso <code>sns:ListSubscriptionsByTopic</code> para el tema de SNS.
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	El resultado se encuentra en un estado de WARNING, porque el tema de SNS asociado a esta regla se encuentra en una región o cuenta diferente. Esta regla no admite comprobaciones entre regiones ni entre cuentas. Se recomienda deshabilitar este control en esta región o cuenta. Ejecútelo solo en la región o cuenta donde se encuentra el recurso.
SNS_TOPIC_INVALID	FAILED	El tema de SNS asociado a esta regla no es válido.
THROTTLING_ERROR	NOT_AVAILABLE	La operación de la API relevante superó la tasa permitida.

ProductFields detalles de los hallazgos de control

Cuando Security Hub CSPM ejecuta comprobaciones de seguridad y genera resultados de control, el [ProductFields](#) atributo de ASFF incluye los siguientes campos:

ArchivalReasons:0/Description

Describe por qué Security Hub CSPM ha archivado las conclusiones existentes.

Por ejemplo, Security Hub CSPM archiva las conclusiones existentes al deshabilitar un control o estándar y al activar o desactivar las [conclusiones de los controles consolidados](#).

ArchivalReasons:0/ReasonCode

Explica el motivo por el que Security Hub CSPM ha archivado las conclusiones existentes.

Por ejemplo, Security Hub CSPM archiva las conclusiones existentes al deshabilitar un control o estándar y al activar o desactivar las [conclusiones de los controles consolidados](#).

StandardsGuideArn o StandardsArn

El ARN del estándar asociado con el control.

Para el estándar de referencia de CIS AWS Foundations, el campo es. StandardsGuideArn

Para los estándares PCI DSS y AWS Foundational Security Best Practices, el campo es. StandardsArn

Estos campos se eliminan en favor de Compliance.AssociatedStandards si habilita los [resultados de control consolidados](#).

StandardsGuideSubscriptionArn o StandardsSubscriptionArn

El ARN de la suscripción de la cuenta al estándar.

Para el estándar de referencia de CIS AWS Foundations, el campo es. StandardsGuideSubscriptionArn

Para los estándares PCI DSS y AWS Foundational Security Best Practices, el campo es. StandardsSubscriptionArn

Estos campos se eliminan si habilita los [resultados de control consolidados](#).

RuleId o ControlId

El identificador del control.

Para el estándar de referencia de CIS AWS Foundations, el campo es `RuleId`.

Para otros estándares, el campo es `ControlId`.

Estos campos se eliminan en favor de `Compliance.SecurityControlId` si habilita los [resultados de control consolidados](#).

`RecommendationUrl`

La dirección URL de la información de corrección del control. Este campo se elimina a favor de `Remediation.Recommendation.Url` si habilita los [resultados de control consolidados](#).

`RelatedAWSResources:0/name`

El nombre del recurso asociado a el resultado.

`RelatedAWSResource:0/type`

El tipo de recurso asociado con el control.

`StandardsControlArn`

El ARN del control. Este campo se elimina si habilita los [resultados de control consolidados](#).

`aws/securityhub/ProductName`

Para los hallazgos basados en el control, el nombre del producto es Security Hub CSPM.

`aws/securityhub/CompanyName`

En el caso de los resultados basados en el control, el nombre de la empresa es AWS.

`aws/securityhub/annotation`

Una descripción del problema descubierto por el control.

`aws/securityhub/FindingId`

El identificador del resultado. Este campo no hace referencia a un estándar si habilita los [resultados de control consolidados](#).

Niveles de gravedad de los hallazgos de control

La gravedad asignada a un control CSPM de Security Hub identifica la importancia del control. La gravedad de un control determina la etiqueta de gravedad asignada a los resultados del control.

Criterios de gravedad

La gravedad de un control se determina en función de la evaluación de los siguientes criterios:

- ¿Cómo de difícil es para un agente de amenazas aprovechar la debilidad de la configuración asociada al control?

La dificultad viene determinada por el grado de sofisticación o complejidad que se requiere para utilizar la debilidad para llevar a cabo un escenario de amenaza.

- ¿Qué probabilidades hay de que la debilidad comprometa sus recursos Cuentas de AWS o sus recursos?

Si sus recursos de Cuentas de AWS ven comprometidos, la confidencialidad, la integridad o la disponibilidad de sus datos o AWS infraestructura se ven afectadas de alguna manera.

La probabilidad de que se ponga en peligro indica la probabilidad de que el escenario de amenaza provoque una interrupción o una violación de sus AWS servicios o recursos.

Como ejemplo, fíjese en las siguientes debilidades de configuración:

- Las claves de acceso de los usuarios no se renuevan cada 90 días.
- Existe la clave de usuario raíz de IAM.

Ambas debilidades son igualmente difíciles de aprovechar para un adversario. En ambos casos, el adversario puede utilizar el robo de credenciales o algún otro método para adquirir una clave de usuario. Luego pueden usarla para acceder a sus recursos de forma no autorizada.

Sin embargo, la probabilidad de que se ponga en peligro es mucho mayor si el autor de la amenaza adquiere la clave de acceso del usuario raíz, ya que esto le da un mayor acceso. Como resultado, la debilidad clave del usuario raíz es más grave.

La gravedad no tiene en cuenta la criticidad del recurso subyacente. El nivel de importancia crítica se define como el nivel de importancia de los recursos que están asociados con el resultado. Por ejemplo, un recurso que está asociado a una aplicación de misión crítica es más crítica que uno asociado a pruebas que no son de producción. Para recopilar información sobre la criticidad de los recursos, utilice el `Criticality` campo del formato de búsqueda de AWS seguridad (ASFF).

La siguiente tabla muestra la dificultad de explotación y la probabilidad de que las etiquetas de seguridad se vean comprometidas.

	Compromiso muy probable	Compromiso probable	Compromiso poco probable	Compromis o muy poco probable
Muy fácil de explotar	Critico	Critico	Alto	Medio
Algo fácil de explotar	Critico	Alto	Medio	Medio
Algo difícil de explotar	Alto	Medio	Medio	Bajo
Muy difícil de explotar	Medio	Medio	Bajo	Bajo

Definiciones de gravedad

Las etiquetas de gravedad se definen de la siguiente manera.

Crítico: el problema debe solucionarse de inmediato para evitar una escalada.

Por ejemplo, un bucket de S3 abierto se considera un hallazgo de gravedad crítica. Debido a que muchos agentes exploran buckets S3 abiertos, es probable que otros detecten los datos de un bucket de S3 expuesto y accedan a ellos.

En general, los recursos que son de acceso público se consideran problemas de seguridad críticos. Debe tratar los resultados críticos con la máxima urgencia. También debe tener en cuenta la criticidad del recurso.

Alto: el problema debe abordarse con prioridad a corto plazo.

Por ejemplo, si un grupo de seguridad de VPC predeterminado está abierto al tráfico entrante y saliente, se considera de gravedad alta. Es bastante fácil para un actor de amenazas comprometer un VPC mediante este método. También es probable que el actor de la amenaza pueda interrumpir o exfiltrar los recursos una vez que estén en el VPC.

Security Hub CSPM recomienda tratar una detección de gravedad alta como una prioridad a corto plazo. Debe tomar medidas correctivas de inmediato. También debe tener en cuenta la criticidad del recurso.

Medio: el tema debe abordarse como una prioridad a medio plazo.

Por ejemplo, la falta de cifrado de los datos en tránsito se considera un resultado de gravedad media. Se requiere un man-in-the-middle ataque sofisticado para aprovechar esta debilidad. Es decir, es algo difícil. Es probable que algunos datos se vean comprometidos si el escenario de amenaza tiene éxito.

Security Hub CSPM recomienda que investigue el recurso implicado lo antes posible. También debe tener en cuenta la criticidad del recurso.

Bajo: el problema no requiere acción por sí solo.

Por ejemplo, la falta de recopilación de información forense se considera de gravedad baja. Este control puede ayudar a evitar futuros compromisos, pero la ausencia de análisis forense no conduce directamente a un compromiso.

No es necesario tomar medidas inmediatas ante los resultados de baja gravedad, pero pueden proporcionar un contexto si los correlacionas con otros problemas.

Informativo: no se encontró ningún punto débil en la configuración.

En otras palabras, el estado es PASSED, WARNING o NOT AVAILABLE.

No se recomienda ninguna acción. Los resultados informativos ayudan a los clientes a demostrar que están en un estado de conformidad.

Evaluación del estado de cumplimiento y el estado de control

El `Compliance.Status` campo del formato de comprobación de AWS seguridad describe el resultado de una comprobación de control. AWS Security Hub Cloud Security Posture Management (CSPM) utiliza el estado de conformidad de los hallazgos de control para determinar el estado de control general. El estado del control se muestra en la página de detalles de un control de la consola CSPM de Security Hub.

Evaluación del estado de cumplimiento de las conclusiones del CSPM de Security Hub

El estado de conformidad para cada resultado se asigna uno de los siguientes valores:

- **PASSED**— Indica que el control ha superado el control de seguridad del hallazgo. Esto establece automáticamente el `CSPM Workflow.Status` de Security Hub en `RESOLVED`

- **FAILED**— Indica que el control no pasó el control de seguridad del hallazgo.
- **WARNING**— Indica que Security Hub CSPM no puede determinar si el recurso está en estado **PASSED** o **FAILED**. Por ejemplo, el [registro AWS Config de recursos](#) no está activado para el tipo de recurso correspondiente.
- **NOT_AVAILABLE**— Indica que la comprobación no se puede completar porque se ha producido un error en el servidor, se ha eliminado el recurso o se ha producido el resultado de la AWS Config evaluación **NOT_APPLICABLE**. Si el resultado AWS Config de la evaluación fue **NOT_APPLICABLE**, Security Hub CSPM archiva automáticamente el hallazgo.

Si el estado de conformidad de un hallazgo cambia de **PASSED** a **FAILED**

WARNING **NOT_AVAILABLE**, o `Workflow.Status` fue o bien **NOTIFIED** o **RESOLVED**, Security Hub CSPM cambia `Workflow.Status` automáticamente a **NEW**

Si no dispone de los recursos correspondientes a un control, Security Hub CSPM produce un **PASSED** hallazgo a nivel de cuenta. Si tiene un recurso correspondiente a un control, pero luego lo elimina, Security Hub CSPM crea un **NOT_AVAILABLE** hallazgo y lo archiva inmediatamente. Transcurridas 18 horas, recibirá un **PASSED** resultado porque ya no dispone de los recursos correspondientes al control.

Obtención del estado de control a partir del estado de conformidad

Security Hub CSPM obtiene un estado de control general a partir del estado de cumplimiento de las conclusiones del control. Al determinar el estado del control, Security Hub CSPM ignora los hallazgos que tienen un `RecordState` de **ARCHIVED** y los hallazgos que tienen un `Workflow.Status` **SUPPRESSED**

El estado de control tiene asignado uno de los siguientes valores:

- **Aprobado**: indica que todos los resultados tienen un estado de conformidad como **PASSED**.
- **Con fallos**: indica que al menos un resultado tiene un estado de conformidad como **FAILED**.
- **Desconocido**: indica que al menos un resultado tiene un estado de conformidad como **WARNING** o **NOT_AVAILABLE**. Ningún resultado tiene un estado de conformidad como **FAILED**.
- **Sin datos**: indica que no hay ningún resultado para el control. Por ejemplo, un control recién habilitado tiene este estado hasta que Security Hub CSPM comience a generar resultados para él. Un control también tiene este estado si todos sus resultados están **SUPPRESSED** o no están disponibles en el estado actual. Región de AWS

- **Desactivado:** indica que el control está desactivado en la cuenta actual y en la región. No se están realizando controles de seguridad para este control en la cuenta y la región actuales. Sin embargo, los resultados de un control desactivado pueden tener un valor para el estado de conformidad hasta 24 horas después de la desactivación.

En el caso de una cuenta de administrador, el estado de control refleja el estado de control de la cuenta de administrador y de las cuentas de los miembros. En concreto, el estado general de un control aparece como Con fallos si el control tiene uno o más resultados fallidos en la cuenta del administrador o en cualquiera de las cuentas de los miembros. Si estableció una región de agregación, el estado de control de la región de agregación refleja el estado de control de dicha región y las regiones vinculadas. En concreto, el estado general de un control aparece como Con fallos si el control tiene uno o más resultados fallidos en la región de agregación o en cualquiera de las regiones vinculadas.

El Security Hub CSPM normalmente genera el estado de control inicial 30 minutos después de la primera visita a la página de resumen o a la página de normas de seguridad de la consola CSPM de Security Hub. El [registro de recursos de AWS Config](#) debe estar configurado para que aparezca el estado de control. Una vez que se generan los estados de control por primera vez, Security Hub CSPM actualiza los estados de control cada 24 horas en función de los resultados de las 24 horas anteriores. Una marca de tiempo en la página de detalles de control indica cuándo se actualizó por última vez el estado de control.

Note

Después de habilitar un control por primera vez, los estados de control pueden tardar hasta 24 horas en generarse en las regiones de China y en. AWS GovCloud (US) Region

Calcular las puntuaciones de seguridad

En la consola AWS Security Hub Cloud Security Posture Management (CSPM), las páginas Resumen y Controles muestran un resumen de la puntuación de seguridad de todos los estándares habilitados. En la página de estándares de seguridad, Security Hub CSPM también muestra una puntuación de seguridad del 0 al 100 por ciento para cada estándar habilitado.

Al activar Security Hub CSPM por primera vez, Security Hub CSPM calcula la puntuación de seguridad resumida y las puntuaciones de seguridad estándar a los 30 minutos de su primera

visita a la página [Resumen o normas de seguridad de la consola](#). Las puntuaciones se generan únicamente para los estándares que están activados al visitar esas páginas en la consola. Además, se debe configurar el registro de AWS Config recursos para que aparezcan las partituras. La puntuación de seguridad resumida es el promedio de las puntuaciones de seguridad estándar. Para revisar una lista de estándares que están habilitados actualmente, puede utilizar el [GetEnabledStandards](#) funcionamiento de la API CSPM de Security Hub.

Tras la primera generación de puntuaciones, Security Hub CSPM actualiza las puntuaciones de seguridad cada 24 horas. Security Hub CSPM muestra una marca de tiempo para indicar cuándo se actualizó por última vez una puntuación de seguridad. Tenga en cuenta que las puntuaciones de seguridad por primera vez pueden tardar hasta 24 horas en generarse en las regiones de China y AWS GovCloud (US) Regions.

Si activas las [conclusiones de control consolidadas](#), tus puntuaciones de seguridad pueden tardar hasta 24 horas en actualizarse. Además, al habilitar una nueva región de agregación o actualizar las regiones vinculadas, se restablecen las puntuaciones de seguridad existentes. Security Hub CSPM puede tardar hasta 24 horas en generar nuevas puntuaciones de seguridad que incluyan datos de las regiones actualizadas.

Método de cálculo de las puntuaciones de seguridad

La puntuación de seguridad representa la proporción de controles superados frente a los controles habilitados. La puntuación se muestra como un porcentaje redondeado hacia arriba o hacia abajo hasta el número entero más cercano.

Security Hub CSPM calcula una puntuación de seguridad resumida para todos los estándares habilitados. Security Hub CSPM también calcula una puntuación de seguridad para cada estándar habilitado. Para calcular la puntuación, los controles habilitados incluyen los controles con los estados Aprobado, Con fallos y Desconocido. Los controles cuyo estado es Sin datos se excluyen del cálculo de la puntuación.

Security Hub CSPM ignora los hallazgos archivados y suprimidos al calcular el estado del control. Esto puede afectar a las puntuaciones de seguridad. Por ejemplo, si suprime todos los resultados fallidos de un control, su estado pasa a ser Aprobado, lo que a su vez puede mejorar sus puntuaciones de seguridad. Para obtener más información sobre el estado de control, consulte [Evaluación del estado de cumplimiento y el estado de control](#).

Ejemplo de puntuación:

Estándar	Controles superados	Controles con errores	Controles desconocidos	Puntuación estándar
AWS Mejores prácticas fundamentales de seguridad, versión 1.0.0	168	22	0	88%
Referencia sobre los AWS fundamentos de la CEI, versión 1.4.0	8	29	0	22%
Índice de referencia sobre AWS los fundamentos de la CEI v1.2.0	6	35	0	15%
Publicación especial 800-53 del NIST, revisión 5	159	56	0	74%
PCI DSS v3.2.1	28	17	0	62%

Al calcular la puntuación de seguridad resumida, Security Hub CSPM cuenta cada control solo una vez en todos los estándares. Por ejemplo, si ha habilitado un control que se aplica a tres estándares habilitados, solo cuenta como un control habilitado a efectos de puntuación.

En este ejemplo, aunque el número total de controles habilitados en todos los estándares habilitados es de 528, Security Hub CSPM cuenta cada control único solo una vez con fines de puntuación. Es probable que el número de controles habilitados únicos sea inferior a 528. Si suponemos que el número de controles habilitados únicos es 515 y el número de controles únicos aprobados es 357,

la puntuación resumida es del 69 %. Esta puntuación se calcula dividiendo el número de controles únicos aprobados entre el número de controles únicos habilitados.

Es posible que tenga una puntuación resumida diferente de la puntuación de seguridad estándar, incluso si solo ha activado un estándar en su cuenta en la región actual. Esto puede ocurrir si ha iniciado sesión en una cuenta de administrador y las cuentas de los miembros tienen habilitados estándares adicionales o estándares diferentes. Esto también puede ocurrir si estás consultando la puntuación de la región de agregación y hay estándares adicionales o diferentes habilitados en las regiones vinculadas.

Puntuaciones de seguridad para las cuentas de administrador

Si ha iniciado sesión en una cuenta de administrador, la puntuación de seguridad resumida y la puntuación estándar representan los estados de control de la cuenta de administrador y de todas las cuentas de los miembros.

Si el estado de un control es Con fallos incluso en la cuenta de un miembro, su estado es Con fallos en la cuenta de administrador y afecta a las puntuaciones de la cuenta de administrador.

Si ha iniciado sesión en una cuenta de administrador y está consultando las puntuaciones de una región de agregación, las puntuaciones de seguridad representan los estados de control de todas las cuentas de los miembros y de todas las regiones vinculadas.

Puntuaciones de seguridad si ha establecido una región de agregación

Si ha establecido una agregación Región de AWS, la puntuación de seguridad resumida y las puntuaciones estándar representan los estados de control en todas las regiones vinculadas.

Si el estado de un control es Con fallos incluso en una región vinculada, su estado es Con fallos en la región de agregación y afecta a las puntuaciones de la región de agregación.

Si ha iniciado sesión en una cuenta de administrador y está consultando las puntuaciones de una Región de agregación, las puntuaciones de seguridad representan los estados de control de todas las cuentas de los miembros y de todas las regiones vinculadas.

Categorías de control en Security Hub CSPM

A cada control se le asigna una categoría. La categoría de un control refleja la función de seguridad a la que se aplica el control.

El valor de la categoría contiene la categoría, la subcategoría dentro de la categoría y, opcionalmente, un clasificador dentro de la subcategoría. Por ejemplo:

- Identificación > Inventario
- Proteger > Protección de datos > Cifrado de datos en tránsito

Estas son las descripciones de las categorías, subcategorías y clasificadores disponibles.

Identificar

Desarrollar la comprensión organizativa para administrar el riesgo de ciberseguridad para sistemas, activos, datos y capacidades.

Inventario

¿Ha implementado el servicio las estrategias correctas de etiquetado de recursos? ¿Las estrategias de etiquetado incluyen al propietario del recurso?

¿Qué recursos utiliza el servicio? ¿Son recursos aprobados para este servicio?

¿Tiene visibilidad del inventario aprobado? Por ejemplo, ¿utiliza servicios como Amazon EC2 Systems Manager y Service Catalog?

Registro

¿Ha habilitado de forma segura todos los registros relevantes para el servicio? Los ejemplos de archivos de registros incluyen los siguientes:

- Registros de flujo de Amazon VPC
- Registros de acceso de Elastic Load Balancing
- CloudFront Registros de Amazon
- Amazon CloudWatch Logs
- Registro de Amazon Relational Database Service
- Registros de indexación lentos de Amazon OpenSearch Service
- Rastreo de X-Ray
- AWS Directory Service registros
- AWS Config artículos
- Instantáneas

Protección

Desarrollar y aplicar las protecciones adecuadas para garantizar la prestación de servicios de infraestructura críticos y prácticas de codificación seguras.

Gestión segura del acceso

- ¿Utiliza el servicio las prácticas de menos privilegios en sus políticas de IAM o de recursos?
- ¿Las contraseñas y los secretos son lo suficientemente complejos? ¿Se rotan apropiadamente?
- ¿Utiliza el servicio la autenticación multifactor (MFA)?
- ¿El servicio evita el usuario raíz?
- ¿Las políticas basadas en recursos permiten el acceso público?

Configuración de red segura

- ¿El servicio evita el acceso público y no seguro a la red remota?
- ¿El servicio se utiliza VPCs correctamente? Por ejemplo, ¿se requiere que los trabajos se ejecuten VPCs?
- ¿El servicio segmenta y aísla adecuadamente los recursos confidenciales?

Protección de los datos

- Cifrado de datos en reposo: ¿el servicio cifra los datos en reposo?
- Cifrado de datos en tránsito: ¿el servicio cifra los datos en tránsito?
- Integridad de los datos: ¿el servicio valida la integridad de los datos?
- Protección contra la eliminación de datos: ¿protege el servicio los datos contra la eliminación accidental?
- Administración/Uso de datos: ¿Utiliza servicios como Amazon Macie para rastrear la ubicación de sus datos confidenciales?

Protección de API

- ¿El servicio se utiliza AWS PrivateLink para proteger las operaciones de la API del servicio?

Servicios de protección

¿Los servicios de protección adecuados están bien ubicados? ¿Proporcionan la cantidad correcta de cobertura?

Los servicios de protección le ayudan a desviar los ataques y compromisos dirigidos al servicio. Algunos ejemplos de servicios de protección AWS incluyen AWS Control Tower, AWS WAF, AWS Shield Advanced, Vanta, Secrets Manager, IAM Access Analyzer y AWS Resource Access Manager.

Desarrollo seguro

¿Utiliza prácticas de codificación seguras?

¿Evita vulnerabilidades como el Top Ten de Open Web Application Security Project (OWASP)?

Detect

Desarrolle e implemente las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad.

Servicios de detección

¿Existen los servicios de detección correctos?

¿Proporcionan la cantidad correcta de cobertura?

Algunos ejemplos de servicios de AWS detección incluyen Amazon GuardDuty, AWS Security Hub Cloud Security Posture Management (CSPM), Amazon Inspector, Amazon Detective, AWS IoT Device Defender, Amazon CloudWatch Alarms y AWS Trusted Advisor.

Respuesta

Desarrolle e implemente las actividades apropiadas para tomar medidas relacionadas con la detección de un evento de ciberseguridad.

Medidas de respuesta

¿Responde rápidamente a los eventos de seguridad?

¿Tiene hallazgos críticos o de alta gravedad activos?

Forenses

¿Puede adquirir datos forenses de forma segura para el servicio? Por ejemplo, ¿adquiere instantáneas de Amazon EBS asociadas con verdaderos resultados positivos?

¿Has creado una cuenta forense?

Recuperar

Desarrolle e implemente las actividades apropiadas para mantener planes de resiliencia y restaurar cualquier capacidad o servicio que se haya visto afectado debido a un evento de ciberseguridad.

Resiliencia

¿La configuración del servicio admite conmutaciones por error elegantes, escalado elástico y alta disponibilidad?

¿Has establecido copias de seguridad?

Revisión de los detalles de los controles en Security Hub (CSPM)

Al seleccionar un control en la página Controles o en la página de detalles estándar de la consola CSPM de Security Hub, accederá a una página de detalles del control.

En la parte superior de la página de detalles del control se indica el estado del control. El estado de control resume el rendimiento de un control en función del estado de conformidad de los resultados del control. El Security Hub CSPM normalmente genera el estado de control inicial 30 minutos después de la primera visita a la página de resumen o a la página de normas de seguridad de la consola CSPM de Security Hub. Los estados solo están disponibles para los controles que están habilitados al visitar esas páginas.

La página de detalles del control también proporciona un desglose del estado de conformidad de los resultados del control en las últimas 24 horas. Para obtener más información sobre el estado de control y el estado de conformidad, consulte [Evaluación del estado de cumplimiento y el estado de control](#).

AWS Config el registro de recursos debe estar configurado para que aparezca el estado de control. Una vez que se generan los estados de control por primera vez, Security Hub CSPM actualiza el estado del control cada 24 horas en función de los resultados de las 24 horas anteriores.

Las cuentas de administrador ven un estado de control agregado en la cuenta de administrador y en las cuentas de los miembros. Si ha establecido una región de agregación, el estado de control incluye los resultados de todas las regiones vinculadas. Para obtener más información sobre el estado de control, consulte [the section called “Estado de conformidad y el estado de control”](#).

También puede activar o desactivar el control desde la página de detalles de control.

 Note

Una vez activado un control, pueden pasar hasta 24 horas hasta que se generen los estados de control por primera vez en las regiones de China y de AWS GovCloud (US) Regions.

La pestaña Estándares y requisitos enumera los estándares para los que se puede habilitar un control y los requisitos relacionados con el control desde diferentes marcos de cumplimiento.

La pestaña Comprobaciones muestra los resultados activos del control de las últimas 24 horas. Los resultados de control se generan cuando Security Hub CSPM ejecuta comprobaciones de seguridad para el control. La lista de esta pestaña no incluye los resultados archivados.

Para cada resultado, la lista proporciona acceso a los detalles del resultado, como el estado de cumplimiento y el recurso relacionado. También puede configurar el estado del flujo de trabajo de cada resultado y enviar los resultados a acciones personalizadas. Para obtener más información, consulte [the section called “Revisión y gestión de los hallazgos de control”](#).

Visualización de detalles de un control

Elige el método de acceso que prefieras y sigue estos pasos para revisar los detalles de un control. Los detalles se aplican a la cuenta corriente y a la región e incluyen lo siguiente:

- El título y la descripción del control.
- Un enlace a una guía de corrección para los hallazgos de un control fallido.
- La gravedad del control.
- Estado del control.

En la consola, también puedes consultar una lista de los hallazgos recientes relacionados con el control. Para hacerlo mediante programación, puede utilizar el [GetFindings](#) funcionamiento de la API CSPM de Security Hub.

Security Hub CSPM console

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Control.
3. Seleccione un control.

Security Hub CSPM API

1. Ejecute [ListSecurityControlDefinitions](#) y proporcione uno o más estándares ARNs para obtener una lista de controles IDs para ese estándar. Para obtener el estándar ARNs, ejecute [DescribeStandards](#). Si no proporciona un ARN estándar, esta API devuelve todo el control CSPM de Security Hub. IDs Esta API devuelve un control de seguridad independiente de los estándares IDs, no el control IDs basado en estándares que existía antes de la publicación de estas funciones.

Ejemplo de solicitud:

```
{
  "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-
  best-practices/v/1.0.0"
}
```

2. Ejecute [BatchGetSecurityControls](#) para obtener detalles sobre uno o más controles de la versión actual y. Cuenta de AWS Región de AWS

Ejemplo de solicitud:

```
{
  "SecurityControlIds": ["Config.1", "IAM.1"]
}
```

AWS CLI

1. Ejecute el [list-security-control-definitions](#) comando y proporcione uno o más estándares ARNs para obtener una lista de controles IDs. Para obtener el estándar ARNs, ejecute el `describe-standards` comando. Si no proporciona un ARN estándar, este comando devuelve todo el control CSPM de Security Hub. IDs Este comando devuelve

un control de seguridad independiente de los estándares IDs, no el control IDs basado en estándares que existía antes de las versiones de estas funciones.

```
aws securityhub --region us-east-1 list-security-control-definitions --  
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-  
security-best-practices/v/1.0.0"
```

2. Ejecute el comando [batch-get-security-controls](#) para obtener detalles sobre uno o más controles de en las Región de AWS y Cuenta de AWS actuales.

```
aws securityhub --region us-east-1 batch-get-security-controls --security-  
control-ids '["Config.1", "IAM.1"]'
```

Controles de filtrado y clasificación en Security Hub CSPM

En la consola AWS Security Hub Cloud Security Posture Management (CSPM), puede utilizar la página Controles para revisar una tabla de los controles que están disponibles en la versión actual. Región de AWS La excepción es una región de agregación. Si [ha configurado una región de agregación](#) e inicia sesión en esa región, la consola muestra los controles que están disponibles en la región de agregación o en una o más regiones vinculadas.

Para centrarse en un subconjunto específico de controles, puede ordenar y filtrar la tabla de controles. Las opciones Filtrar por situadas junto a la tabla pueden ayudarle a centrarse rápidamente en estos subconjuntos específicos:

- Todos los controles habilitados, que son controles que están habilitados en al menos un estándar habilitado.
- Todos los controles deshabilitados, que son controles que están deshabilitados en todos los estándares.
- Todos los controles activados que tienen un estado de control específico, como Fallido. La opción Sin datos muestra solo los controles que actualmente no tienen resultados. Para obtener información sobre el estado de los controles, consulte [Evaluación del estado de cumplimiento y el estado de control](#).

Además de las opciones Filtrar por, puede filtrar la tabla introduciendo los criterios de filtrado en el cuadro de controles de filtrado situado encima de la tabla. Por ejemplo, puede filtrar por ID de control o gravedad.

De forma predeterminada, los controles con el estado Error aparecen primero, en orden descendente por gravedad. Puede cambiar el orden de clasificación eligiendo un encabezado de columna diferente.

 Tip

Si ha automatizado los flujos de trabajo en función de los resultados de los controles, le recomendamos que utilice los [campos SecurityControlId o SecurityControlArn ASFF](#) como filtros, en lugar de los Description campos Title o. Estos últimos campos pueden cambiar de vez en cuando, mientras que el ID de control y el ARN son identificadores estáticos.

Si ha iniciado sesión en una cuenta de administrador CSPM de Security Hub, los controles habilitados incluyen los controles que están habilitados en al menos una cuenta de miembro. Si ha configurado una región de agregación, los controles habilitados incluyen los controles que están habilitados en al menos una región vinculada.

Si selecciona la opción situada junto a un control activado, aparece un panel que muestra los estándares en los que el control está activado actualmente. También puede ver los estándares en los que el control está actualmente desactivado. Desde este panel, puede deshabilitar un control en todos los estándares. Para obtener más información, consulte [Desactivación de los controles en Security Hub \(CSPM\)](#). En el caso de las cuentas de administrador, la información del panel refleja la configuración de todas sus cuentas de miembros.

Para recuperar una lista de controles mediante programación, puede utilizar el [ListSecurityControlDefinitions](#) funcionamiento de la API CSPM de Security Hub. Para recuperar los detalles de los controles individuales, utilice la operación. [BatchGetSecurityControls](#)

Descripción de los parámetros de control en Security Hub CSPM

Algunos controles de AWS Security Hub Cloud Security Posture Management (CSPM) utilizan parámetros que afectan a la forma en que se evalúa el control. Normalmente, estos controles se evalúan con respecto a los valores de los parámetros predeterminados que define Security Hub

CSPM. Sin embargo, para un subconjunto de estos controles, puede modificar los valores de los parámetros. Al modificar el valor de un parámetro de control, Security Hub CSPM comienza a evaluar el control con respecto al valor que especifique. Si el recurso subyacente al control cumple con el valor personalizado, Security Hub CSPM genera un hallazgo. PASSED Si el recurso no cumple con el valor personalizado, Security Hub CSPM genera un FAILED hallazgo.

Al personalizar los parámetros de control, puede refinar las mejores prácticas de seguridad recomendadas y supervisadas por Security Hub CSPM para alinearlas con los requisitos empresariales y las expectativas de seguridad. En lugar de suprimir los resultados de un control, puede personalizar uno o varios de sus parámetros para obtener los resultados que se adapten a sus necesidades de seguridad.

Estos son algunos ejemplos de casos de uso para modificar los parámetros de control y establecer valores personalizados:

- [CloudWatch.16]: los grupos de CloudWatch registros deben conservarse durante un período de tiempo específico

Puede especificar el periodo de retención.

- [IAM.7]: las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras

Puede especificar parámetros relacionados con la seguridad de la contraseña.

- [EC2.18] — Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados

Puede especificar qué puertos están autorizados para permitir el tráfico entrante sin restricciones.

- [Lambda.5]: las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad

Puede especificar el número mínimo de zonas de disponibilidad que generará un resultado válido.

En esta sección, se describen los aspectos que se deben tener en cuenta al modificar los parámetros de control.

Efecto de la modificación de los valores de parámetros de control

Al cambiar el valor de un parámetro, también se desencadena un nuevo control de seguridad que evalúa el control en función del nuevo valor. A continuación, Security Hub CSPM genera nuevos hallazgos de control en función del nuevo valor. Durante las actualizaciones periódicas de los

hallazgos de control, Security Hub CSPM también utiliza el nuevo valor del parámetro. Si cambia los valores de los parámetros de un control, pero no ha activado ningún estándar que incluya el control, Security Hub CSPM no realizará ninguna comprobación de seguridad con los nuevos valores. Debe habilitar al menos un estándar relevante para que Security Hub CSPM evalúe el control en función del nuevo valor del parámetro.

Un control puede tener uno o varios parámetros personalizables. Entre los tipos de datos posibles para cada parámetro de control se encuentran los siguientes:

- Booleano
- Doble
- Enum
- EnumList
- Entero
- IntegerList
- Cadena
- StringList

Los valores personalizados de los parámetros se aplican a los estándares habilitados. No puede personalizar los parámetros de un control que no sea compatible en su región actual. Para obtener una lista de los límites regionales para los controles individuales, consulte [Límites regionales de los controles CSPM de Security Hub](#).

En algunos controles, los valores de los parámetros aceptables deben estar dentro de un rango especificado para ser válidos. En estos casos, Security Hub CSPM proporciona el rango aceptable.

Security Hub CSPM elige los valores de los parámetros predeterminados y puede que los actualice de vez en cuando. Después de personalizar un parámetro de control, su valor sigue siendo el valor que especificó para el parámetro, a menos que lo cambie. Es decir, el parámetro detiene el seguimiento de las actualizaciones del valor CSPM predeterminado del Security Hub, incluso si el valor personalizado del parámetro coincide con el valor predeterminado actual definido por el CSPM del Security Hub. Este es un ejemplo del control [ACM.1]: los certificados importados y emitidos por ACM deben renovarse después de un periodo de tiempo específico:

```
{  
  "SecurityControlId": "ACM.1",
```

```
"Parameters": {
  "daysToExpiration": {
    "ValueType": "CUSTOM",
    "Value": {
      "Integer": 30
    }
  }
}
```

En el ejemplo anterior, el parámetro `daysToExpiration` tiene un valor personalizado de 30. El valor predeterminado actual para este parámetro también es 30. Si Security Hub CSPM cambia el valor predeterminado a 14, el parámetro de este ejemplo no rastreará ese cambio. Retendrá un valor de 30.

Si desea realizar un seguimiento de las actualizaciones del valor CSPM predeterminado de Security Hub para un parámetro, defina el `ValueType` campo `DEFAULT` en lugar de `CUSTOM`. Para obtener más información, consulte [Reversión a los parámetros de control predeterminados en una sola cuenta y región](#).

Controles que admiten parámetros personalizados

Para obtener una lista de los controles de seguridad que admiten parámetros personalizados, consulte la página de controles de la consola CSPM de Security Hub o la [Referencia de control para Security Hub CSPM](#). Para recuperar esta lista mediante programación, puede utilizar la operación [ListSecurityControlDefinitions](#). En la respuesta, el objeto `CustomizableProperties` indica qué controles admiten parámetros personalizables.

Revisión de los valores actuales de los parámetros de control

Puede resultar útil conocer el valor actual de un parámetro de control antes de modificarlo.

Puede revisar los valores actuales de los parámetros de control individuales de su cuenta. Si utiliza la configuración central, el administrador delegado de AWS Security Hub Cloud Security Posture Management (CSPM) también puede revisar los valores de los parámetros que se especifican en una política de configuración.

Elija el método que prefiera y siga los pasos para revisar los valores actuales de los parámetros de control.

Security Hub CSPM console

Para revisar los valores actuales de los parámetros de control (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Controles. Elija un control.
3. Elija la pestaña Parámetros. Esta pestaña muestra los valores actuales de los parámetros del control.

Security Hub CSPM API

Para revisar los valores actuales de los parámetros de control (API)

invoque la [BatchGetSecurityControls](#) API y proporcione uno o más controles de seguridad o. IDs ARNs El objeto Parameters de la respuesta muestra los valores actuales de los parámetros de los controles especificados.

Por ejemplo, el siguiente AWS CLI comando muestra los valores de los parámetros actuales para APIGateway.1CloudWatch.15, yIAM.7. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

Elija el método que prefiera para ver los valores actuales de los parámetros en una política de configuración centralizada.

Security Hub CSPM console

Para revisar los valores actuales de los parámetros de control en una política de configuración (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>

Inicie sesión con las credenciales de la cuenta de administrador CSPM de Security Hub delegada en la región de origen.

2. En el panel de navegación, seleccione Configuración y Configuración.
3. En la pestaña Políticas, seleccione la política de configuración y, a continuación, elija Ver detalles. A continuación, aparecen los detalles de la política, incluidos los valores actuales de los parámetros.

Security Hub CSPM API

Para revisar los valores actuales de los parámetros de control en una política de configuración (API)

1. Invoque la API [GetConfigurationPolicy](#) desde la cuenta de administrador delegado de la región de origen.
2. Proporcione el ARN o el ID de la política de configuración cuyos detalles quiere ver. La respuesta incluye los valores actuales de los parámetros.

Por ejemplo, el siguiente AWS CLI comando recupera los valores de los parámetros de control actuales de la política de configuración especificada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Los resultados de control también incluyen los valores actuales de los parámetros de control. En la [AWS Formato de búsqueda de seguridad \(ASFF\)](#), estos valores aparecen en el campo Parameters del objeto Compliance. Para revisar los resultados en la consola CSPM de Security Hub, seleccione Resultados en el panel de navegación. Para revisar los hallazgos mediante programación, utilice la [GetFindings](#) operación de la API CSPM de Security Hub.

Personalización de los valores de los parámetros de control

Las instrucciones para personalizar los parámetros de control varían en función de si se utiliza la [configuración central](#) en AWS Security Hub Cloud Security Posture Management (CSPM). La configuración central es una función que el administrador de CSPM del Security Hub delegado puede utilizar para configurar las capacidades de CSPM del Security Hub en todas las cuentas y unidades Regionales de AWS organizativas (). OUs

Si su organización utiliza la configuración central, el administrador delegado puede crear políticas de configuración que incluyan parámetros de control personalizados. Estas políticas se pueden asociar a las cuentas de los miembros administradas de forma centralizada y entran OUs en vigor en su región de origen y en todas las regiones vinculadas. El administrador delegado también puede designar una o varias cuentas como autoadministradas, lo que permite al propietario de la cuenta configurar sus propios parámetros por separado en cada región. Si su organización no utiliza la configuración centralizada, debe personalizar los parámetros de control por separado en cada cuenta y región.

Recomendamos utilizar la configuración centralizada porque permite alinear los valores de los parámetros de control en las distintas partes de la organización. Por ejemplo, todas sus cuentas de prueba podrían usar determinados valores de parámetros y todas las cuentas de producción podrían utilizar valores diferentes.

Personalización de parámetros de control en varias cuentas y regiones

Si es el administrador delegado de CSPM de Security Hub para una organización que utiliza una configuración central, elija el método que prefiera y siga los pasos para personalizar los parámetros de control en varias cuentas y regiones.

Security Hub CSPM console

Para personalizar los valores de un parámetro de control en varias cuentas y regiones (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>

Asegúrese de que haya iniciado sesión en la región de origen.

2. En el panel de navegación, seleccione Configuración y Configuración.
3. Elija la pestaña Políticas.

4. Para crear una nueva política de configuración que incluya parámetros personalizados, elija Crear política. Para especificar los parámetros personalizados en una política de configuración existente, seleccione la política y, luego, elija Editar.

Para crear una política de configuración nueva con valores de parámetros de control personalizados

1. En la sección Política personalizada, elija los estándares y controles de seguridad que quiere habilitar.
2. Seleccione Personalizar los parámetros de control.
3. Seleccione un control y, a continuación, especifique valores personalizados para uno o varios parámetros.
4. Para personalizar los parámetros de más controles, elija Personalizar un control adicional.
5. En la sección Cuentas, selecciona las cuentas a las que quieres aplicar la política o las cuentas a las OUs que quieres aplicar la política.
6. Elija Siguiente.
7. Elija Crear y aplicar política. En su región de origen y en todas las regiones vinculadas, esta acción anula los ajustes de configuración existentes de las cuentas y OUs que están asociados a esta política de configuración. Cuenta y se OUs puede asociar a una política de configuración mediante una aplicación directa o mediante herencia de un padre.

Para personalizar los valores de un parámetro de control en una política de configuración existente

1. En la sección Controles, en Política personalizada, especifique los nuevos valores personalizados de parámetros que quiera.
2. Si es la primera vez que personaliza los parámetros de control en esta política, seleccione Personalizar los parámetros de control y, a continuación, seleccione el control que quiere personalizar. Para personalizar los parámetros de más controles, elija Personalizar un control adicional.
3. En la sección Cuentas, verifica las cuentas a las OUs que deseas aplicar la política o las cuentas a las que deseas aplicar la política.
4. Elija Siguiente.
5. Revise los cambios y compruebe que sean correctos. Cuando termine, elija Guardar y aplicar política. En su región de origen y en todas las regiones vinculadas, esta acción

anula los ajustes de configuración existentes de las cuentas y OUs que están asociados a esta política de configuración. Cuenta y se OUs puede asociar a una política de configuración mediante una aplicación directa o mediante herencia de un padre.

Security Hub CSPM API

Para personalizar los valores de un parámetro de control en varias cuentas y regiones (API)

Para crear una política de configuración nueva con valores de parámetros de control personalizados

1. Invoque la API [CreateConfigurationPolicy](#) desde la cuenta de administrador delegado de la región de origen.
2. Para el objeto `SecurityControlCustomParameters`, indique el identificador de cada control que quiere personalizar.
3. Para el objeto `Parameters`, indique el nombre de cada parámetro que quiere personalizar. Para cada parámetro que personalice, indique `CUSTOM` en `ValueType`. En `Value`, indique el tipo de datos del parámetro y el valor personalizado. El campo `Value` no puede estar vacío cuando el valor de `ValueType` es `CUSTOM`. Si la solicitud omite un parámetro que el control admite, ese parámetro conserva su valor actual. Para encontrar los parámetros, los tipos de datos y los valores válidos admitidos para un control, invoque la API [GetSecurityControlDefinition](#).

Para personalizar los valores de un parámetro de control en una política de configuración existente

1. Invoque la API [UpdateConfigurationPolicy](#) desde la cuenta de administrador delegado de la región de origen.
2. En el campo `Identifier`, indique el nombre de recurso de Amazon (ARN) o el identificador de la política de configuración que quiera actualizar.
3. Para el objeto `SecurityControlCustomParameters`, indique el identificador de cada control que quiere personalizar.
4. Para el objeto `Parameters`, indique el nombre de cada parámetro que quiere personalizar. Para cada parámetro que personalice, indique `CUSTOM` en `ValueType`. En `Value`, indique el tipo de datos del parámetro y el valor personalizado. Si la solicitud omite un parámetro que el control admite, ese parámetro conserva su valor actual. Para encontrar los

parámetros, los tipos de datos y los valores válidos admitidos para un control, invoque la API [GetSecurityControlDefinition](#).

Por ejemplo, el siguiente AWS CLI comando crea una nueva política de configuración con un valor personalizado para el `daysToExpiration` parámetro de `ACM.1`. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (`\`) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
"EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0","arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0"], "SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
"SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
{"daysToExpiration": {"ValueType": "CUSTOM", "Value": "Integer": 15}}]}}}'
```

Personalización de parámetros de control en una sola cuenta y región

Si no utiliza la configuración centralizada o tiene una cuenta autoadministrada, puede personalizar los parámetros de control de su cuenta en una región a la vez.

Elija el método que prefiera y siga los pasos para personalizar los parámetros de control. Los cambios se aplican solo a su cuenta en la región actual. Para personalizar los parámetros de control en otras regiones, repita los siguientes pasos en cada cuenta o región adicional en la que quiere personalizar los parámetros. El mismo control puede utilizar valores de parámetros diferentes en regiones distintas.

Security Hub CSPM console

Para personalizar los valores de un parámetro de control en una cuenta y región (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>

2. En el panel de navegación, elija Controles. En la tabla, elija un control que admita parámetros personalizados y cuyos parámetros quiere cambiar. La columna Parámetros personalizados indica qué controles los admiten.
3. En la página de detalles del control, seleccione la pestaña Parámetros y, a continuación, elija Editar.
4. Especifique los valores de los parámetros que quiere cambiar.
5. De manera opcional, en la sección Motivo del cambio, seleccione un motivo para personalizar los parámetros.
6. Seleccione Save.

Security Hub CSPM API

Para personalizar los valores de un parámetro de control en una cuenta y región (API)

1. Invoque la API [UpdateSecurityControl](#).
2. En `SecurityControlId`, indique el identificador del control que quiere personalizar.
3. Para el objeto `Parameters`, indique el nombre de cada parámetro que quiere personalizar. Para cada parámetro que personalice, indique `CUSTOM` en `ValueType`. En `Value`, indique el tipo de datos del parámetro y el valor personalizado. Si la solicitud omite un parámetro que el control admite, ese parámetro conserva su valor actual. Para encontrar los parámetros, los tipos de datos y los valores válidos admitidos para un control, invoque la API [GetSecurityControlDefinition](#).
4. De manera opcional, en `LastUpdateReason`, indique un motivo para personalizar los parámetros de control.

Por ejemplo, el siguiente AWS CLI comando define un valor personalizado para el `daysToExpiration` parámetro de `ACM.1`. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (`\`) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":  
15}}}' \
--last-update-reason "Internal compliance requirement"
```

Reversión de los valores predeterminados de los parámetros de control

Un parámetro de control puede tener un valor predeterminado que defina AWS Security Hub Cloud Security Posture Management (CSPM). Ocasionalmente, Security Hub CSPM actualiza el valor predeterminado de un parámetro para reflejar la evolución de las mejores prácticas de seguridad. Si no ha especificado un valor personalizado para un parámetro de control, el control hace un seguimiento automático de esas actualizaciones y utiliza el nuevo valor predeterminado.

Puede volver a utilizar los valores predeterminados del parámetro para un control. Las instrucciones para la reversión dependen de si se utiliza la [configuración central](#) en Security Hub CSPM. La configuración central es una función que el administrador de CSPM del Security Hub delegado puede utilizar para configurar las capacidades de CSPM del Security Hub en todas las cuentas y unidades Regionales de AWS organizativas (). OUs

Note

No todos los parámetros de control tienen un valor CSPM predeterminado de Security Hub. En esos casos, cuando `ValueType` se establece en `DEFAULT`, no hay un valor predeterminado específico que utilice Security Hub CSPM. Por el contrario, Security Hub CSPM ignora el parámetro en ausencia de un valor personalizado.

Reversión a los parámetros de control predeterminados en varias cuentas y regiones

Si utiliza una configuración central, puede revertir los parámetros de control de varias cuentas administradas de forma centralizada y de la región de origen y OUs las regiones vinculadas.

Elija el método que prefiera y siga los pasos para revertir a los valores predeterminados de los parámetros en varias cuentas y regiones mediante la configuración centralizada.

Security Hub CSPM console

Para revertir los valores predeterminados de los parámetros de control en varias cuentas y regiones (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>

Inicie sesión con las credenciales de la cuenta de administrador CSPM de Security Hub delegada en la región de origen.

2. En el panel de navegación, seleccione Configuración y Configuración.
3. Elija la pestaña Políticas.
4. Seleccione una política y, a continuación, elija Editar.
5. En Política personalizada, la sección Controles muestra una lista de controles para los que especificó parámetros personalizados.
6. Busque el control que tenga uno o varios valores de parámetros que revertir. A continuación, elija Eliminar para revertir a los valores predeterminados.
7. En la sección Cuentas, compruebe las cuentas o a las OUs que desea aplicar la política.
8. Elija Siguiente.
9. Revise los cambios y compruebe que sean correctos. Cuando termine, elija Guardar y aplicar política. En su región de origen y en todas las regiones vinculadas, esta acción anula los ajustes de configuración existentes de las cuentas y OUs que están asociados a esta política de configuración. Cuenta y se OUs puede asociar a una política de configuración mediante una aplicación directa o mediante herencia de un padre.

Security Hub CSPM API

Para revertir los valores predeterminados de los parámetros de control en varias cuentas y regiones (API)

1. Invoque la API [UpdateConfigurationPolicy](#) desde la cuenta de administrador delegado de la región de origen.
2. En el campo `Identifier`, indique el nombre de recurso de Amazon (ARN) o el identificador de la política que quiere actualizar.
3. Para el objeto `SecurityControlCustomParameters`, indique el identificador de cada control para revertir uno o varios parámetros.
4. En el objeto `Parameters`, para cada parámetro que quiere revertir, indique `DEFAULT` en el campo `ValueType`. Si `ValueType` está establecido en `DEFAULT`, no es necesario proporcionar un valor para el campo `Value`. Si se incluye un valor en la solicitud, Security Hub CSPM lo ignora. Si la solicitud omite un parámetro que el control admite, ese parámetro conserva su valor actual.

⚠ Warning

Si omite un objeto de control del `SecurityControlCustomParameters` campo, Security Hub CSPM revierte todos los parámetros personalizados del control a sus valores predeterminados. Una lista completamente vacía para `SecurityControlCustomParameters` revierte los parámetros personalizados de todos los controles a sus valores predeterminados.

Por ejemplo, el siguiente AWS CLI comando revierte el parámetro de `daysToExpiration` control for ACM.1 a su valor predeterminado en la política de configuración especificada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--name "TestConfigurationPolicy" \
--description "Updated configuration policy" \
--updated-reason "Revert ACM.1 parameter to default value"
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
"EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0","arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
"SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
{"daysToExpiration": {"ValueType": "DEFAULT"}}]}}}'
```

Reversión a los parámetros de control predeterminados en una sola cuenta y región

Si no utiliza la configuración centralizada o tiene una cuenta autoadministrada, puede revertir al uso de los valores predeterminados de los parámetros para su cuenta en una región a la vez.

Elija el método que prefiera y siga los pasos para revertir a los valores predeterminados de los parámetros para su cuenta en una sola región. Para volver a los valores predeterminados de los parámetros en otras regiones, repita estos pasos en cada región adicional.

 Note

Si deshabilita el CSPM de Security Hub, se restablecen los parámetros de control personalizados. Si vuelve a habilitar el CSPM de Security Hub en el futuro, todos los controles utilizarán los valores de los parámetros predeterminados para comenzar.

Security Hub CSPM console

Para revertir los valores predeterminados de los parámetros de control en una cuenta o región (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Controles. Elija el control que quiere revertir a los valores predeterminados de los parámetros.
3. En la pestaña Parameters, elija Personalizado junto a un parámetro de control. A continuación, seleccione Eliminar personalización. Este parámetro ahora usa el valor CSPM predeterminado de Security Hub y rastrea las actualizaciones futuras hasta el valor predeterminado.
4. Repita el paso anterior para cada valor de parámetro que quiere revertir.

Security Hub CSPM API

Para revertir los valores predeterminados de los parámetros de control en una cuenta o región (API)

1. Invoque la API [UpdateSecurityControl](#).
2. En SecurityControlId, indique el ARN o el identificador del control cuyos parámetros quiere revertir.
3. En el objeto Parameters, para cada parámetro que quiere revertir, indique DEFAULT en el campo ValueType. Si ValueType está establecido en DEFAULT, no es necesario proporcionar un valor para el campo Value. Si se incluye un valor en la solicitud, Security Hub CSPM lo ignora.
4. De manera opcional, en LastUpdateReason, indique un motivo para revertir a los valores predeterminados de los parámetros.

Por ejemplo, el siguiente AWS CLI comando revierte el parámetro de `daysToExpiration` control ACM.1 a su valor predeterminado. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (`\`) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

Comprobación del estado de los cambios de los parámetros de control

Al intentar personalizar un parámetro de control o volver al valor predeterminado, puede validar si los cambios deseados se realizaron correctamente. Esto ayuda a garantizar que un control funcione como se espera y proporcione el valor de seguridad previsto. Si la actualización de un parámetro no se realiza correctamente, Security Hub CSPM conserva el valor actual del parámetro.

Para comprobar que la actualización de los parámetros se ha realizado correctamente, puede revisar los detalles del control en la consola CSPM de Security Hub. En el panel de navegación de la consola, elija Controles. A continuación, elija un control para mostrar sus detalles. La pestaña Parámetros muestra el estado del cambio del parámetro.

Desde el punto de vista programático, si la solicitud de actualización de un parámetro es válida, el valor del campo `UpdateStatus` es `UPDATING` en una respuesta a la operación [BatchGetSecurityControls](#). Esto significa que la actualización era válida, pero es posible que todos los resultados aún no incluyan los valores de los parámetros actualizados. Cuando el valor de `UpdateState` cambia a `READY`, Security Hub CSPM utiliza los valores de los parámetros de control actualizados al ejecutar las comprobaciones de seguridad del control. Los resultados incluyen los valores de los parámetros actualizados.

La operación `UpdateSecurityControl` devuelve una respuesta `InvalidInputException` para los valores de los parámetros no válidos. La respuesta proporciona detalles adicionales sobre el motivo del error. Por ejemplo, es posible que haya especificado un valor que está fuera del rango válido de un parámetro. O bien, es posible que haya especificado un valor que no utiliza el tipo de datos correcto. Vuelva a enviar la solicitud con una entrada válida.

Si se produce un error interno al intentar actualizar el valor de un parámetro, el CSPM de Security Hub lo volverá a intentar automáticamente si lo ha activado. AWS Config Para obtener más información, consulte [Consideraciones antes de habilitar y configurar AWS Config](#).

Revisión y gestión de los resultados de control en Security Hub (CSPM)

La página de detalles del control muestra una lista de los resultados activos de un control. La lista no incluye resultados archivados.

La página de detalles del control admite la agregación entre regiones. Si ha establecido una región de agregación, el estado del control y la lista de controles de seguridad de la página de detalles del control incluyen las comprobaciones de todas las Regiones de AWS vinculadas.

La lista proporciona herramientas para filtrar y ordenar los resultados, de modo que pueda centrarse primero en los más urgentes. Un resultado puede incluir enlaces a información detallada sobre los recursos en la consola de servicio correspondiente. En el caso de los controles que se basan en AWS Config reglas, puede ver los detalles de la regla.

También puede usar la API AWS Security Posture Management (CSPM) de Security Hub Cloud para recuperar una lista de hallazgos y detalles de los hallazgos.

Para obtener más información, consulte [Revisión de los detalles y el historial de resultados](#).

Para reflejar el estado actual de la investigación de un resultado de control, debe configurar el estado del flujo de trabajo. Para obtener más información, consulte [the section called “Configuración del estado de flujo de trabajo de los resultados”](#).

También puedes enviar los resultados de CSPM seleccionados de Security Hub a una acción personalizada en Amazon. EventBridge Para obtener más información, consulte [the section called “Envío de hallazgos a una acción personalizada”](#).

Temas

- [Filtrado y clasificación de resultados de control](#)
- [Muestras de los resultados de los controles](#)

Filtrado y clasificación de resultados de control

Si selecciona un control en la página de controles de la consola AWS Security Hub Cloud Security Posture Management (CSPM) o en la página de detalles de un estándar, accederá a la página de detalles del control.

La página de detalles del control muestra el título y la descripción del control, el estado general del control y un desglose de los controles de seguridad de las últimas 24 horas.

Utilice las opciones Filtrar por situadas junto a la lista de controles de seguridad para centrarse rápidamente en los resultados relacionados con un [estado de flujo de trabajo](#) o un [estado de conformidad](#) específicos.

Además de las opciones Filtrar por, puede usar la casilla Agregar filtro para filtrar la lista de verificación por otros campos, como el Cuenta de AWS ID o el ID del recurso.

Los resultados cuyo estado de conformidad es APROBADO se enumeran en primer lugar de forma predeterminada. Puede cambiar el orden predeterminado si selecciona una opción diferente en los encabezados de las columnas.

En la página de detalles del control, puede seleccionar Descargar para descargar la página actual de resultados de control en un archivo .csv.

Si filtra la lista de resultados, la descarga solo incluirá los controles que coincidan con el filtro. Si selecciona resultados específicos de la lista, la descarga solo incluirá los resultados seleccionados.

Para obtener más información sobre cómo filtrar resultados, consulte [Filtrado de resultados en Security Hub \(CSPM\)](#).

Muestras de los resultados de los controles

Los siguientes ejemplos proporcionan ejemplos de los resultados de control de AWS Security Hub Cloud Security Posture Management (CSPM) en el formato de búsqueda de AWS seguridad (ASFF). El contenido de las conclusiones de control varía en función de si se han activado las conclusiones de control consolidadas.

Si habilita los hallazgos de control consolidados, Security Hub CSPM genera un único hallazgo para un control, incluso si el control se aplica a varios estándares habilitados. Si no habilita esta función, Security Hub CSPM genera un hallazgo de control independiente para cada estándar habilitado al que se aplique un control. Por ejemplo, si habilita dos estándares y se aplica un control a ambos, recibirá dos resultados distintos para el control, uno para cada estándar. Si habilita las conclusiones

de control consolidadas, recibirá solo una conclusión para el control. Para obtener más información, consulte [Resultados de control consolidados](#).

Los ejemplos de esta página proporcionan ejemplos de ambos escenarios. Los ejemplos incluyen: hallazgos de control para estándares CSPM individuales de Security Hub cuando los hallazgos de control consolidados están deshabilitados y un hallazgo de control para varios estándares CSPM de Security Hub cuando los hallazgos de control consolidados están habilitados.

Muestras de los resultados de los controles

- [Ejemplo de hallazgo del estándar AWS Foundational Security Best Practices](#)
- [Ejemplo de hallazgo para CIS AWS Foundations Benchmark v3.0.0](#)
- [Ejemplo de hallazgo para CIS AWS Foundations Benchmark v1.4.0](#)
- [Ejemplo de hallazgo para CIS AWS Foundations Benchmark v1.2.0](#)
- [Ejemplo de hallazgo para la norma NIST SP 800-53, revisión 5](#)
- [Ejemplo de hallazgo de la norma NIST SP 800-171, revisión 2](#)
- [Ejemplo de búsqueda del estándar de seguridad de datos de la industria de tarjetas de pago, versión 3.2.1](#)
- [Ejemplo de hallazgo para el estándar AWS de etiquetado de recursos](#)
- [Ejemplo de hallazgo para el estándar de AWS Control Tower gestión de servicios](#)
- [Ejemplo de hallazgo consolidado para varios estándares](#)

Note

Los resultados de los controles hacen referencia a diferentes campos y valores en las Regiones de China y las AWS GovCloud (US) Regiones. Para obtener más información, consulte [Impacto de la consolidación en los campos y valores ASFF](#).

Ejemplo de hallazgo del estándar AWS Foundational Security Best Practices

El siguiente ejemplo proporciona un ejemplo de la búsqueda de un control que se aplica al estándar AWS Foundational Security Best Practices (FSBP). En este ejemplo, los resultados de control consolidados están deshabilitados.

```
{  
  "SchemaVersion": "2018-10-08",
```

```

    "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
    "ProductName": "Security Hub CSPM",
    "CompanyName": "AWS",
    "Region": "us-east-2",
    "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "AwsAccountId": "123456789012",
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
    ],
    "FirstObservedAt": "2020-08-06T02:18:23.076Z",
    "LastObservedAt": "2021-09-28T16:10:06.956Z",
    "CreatedAt": "2020-08-06T02:18:23.076Z",
    "UpdatedAt": "2021-09-28T16:10:00.093Z",
    "Severity": {
      "Product": 40,
      "Label": "MEDIUM",
      "Normalized": 40,
      "Original": "MEDIUM"
    },
    "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
    "Description": "This AWS control checks whether AWS CloudTrail is configured to use
the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
    "Remediation": {
      "Recommendation": {
        "Text": "For directions on how to correct this issue, consult the AWS Security
Hub Cloud Security Posture Management (CSPM) controls documentation.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
      }
    },
    "ProductFields": {
      "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-
practices/v/1.0.0",
      "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
      "ControlId": "CloudTrail.2",
      "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
      "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",

```

```

    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/Product Name": "Security Hub CSPM",
    "aws/securityhub/Company Name": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
    ]
  }
}

```

}

Ejemplo de hallazgo para CIS AWS Foundations Benchmark v3.0.0

El siguiente ejemplo proporciona un ejemplo de la búsqueda de un control que se aplica a CIS AWS Foundations Benchmark v3.0.0. En este ejemplo, los resultados del control consolidado están desactivados.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS Foundations Benchmark"
  ],
  "FirstObservedAt": "2024-04-18T07:46:18.193Z",
  "LastObservedAt": "2024-04-23T07:47:01.137Z",
  "CreatedAt": "2024-04-18T07:46:18.193Z",
  "UpdatedAt": "2024-04-23T07:46:46.165Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.2.1 EBS default encryption should be enabled",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using the Elastic Block Store (EBS) service. While disabled by default, forcing encryption at EBS volume creation is supported.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  }
},
```

```

"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/cis-aws-foundations-benchmark/
v/3.0.0",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0",
  "ControlId": "2.2.1",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
  "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2843ed9e",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1",
  "aws/securityhub/ProductName": "Security Hub CSPM",
  "aws/securityhub/CompanyName": "AWS",
  "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
  "Resources:0/Id": "arn:aws:iam::123456789012:root",
  "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c"
},
"Resources": [
  {
    "Type": "AwsAccount",
    "Id": "AWS:::Account:123456789012",
    "Partition": "aws",
    "Region": "us-east-1"
  }
],
"Compliance": {
  "Status": "FAILED",
  "RelatedRequirements": [
    "CIS AWS Foundations Benchmark v3.0.0/2.2.1"
  ],
  "SecurityControlId": "EC2.7",
  "AssociatedStandards": [
    {
      "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"
    }
  ]
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},

```

```

"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
  ]
},
"ProcessedAt": "2024-04-23T07:47:07.088Z"
}

```

Ejemplo de hallazgo para CIS AWS Foundations Benchmark v1.4.0

El siguiente ejemplo proporciona un ejemplo de un hallazgo de un control que se aplica a CIS AWS Foundations Benchmark v1.4.0. En este ejemplo, los resultados del control consolidado están desactivados.

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
  ],
  "FirstObservedAt": "2022-10-21T22:14:48.913Z",
  "LastObservedAt": "2022-12-22T22:24:56.980Z",
  "CreatedAt": "2022-10-21T22:14:48.913Z",
  "UpdatedAt": "2022-12-22T22:24:52.409Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  }
}

```

```

},
  "Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS CloudTrail is a web service that records AWS API calls for an
account and makes those logs available to users and resources in accordance with IAM
policies. AWS Key Management Service (KMS) is a managed service that helps create
and control the encryption keys used to encrypt account data, and uses Hardware
Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs
can be configured to leverage server side encryption (SSE) and AWS KMS customer
created master keys (CMK) to further protect CloudTrail logs. It is recommended that
CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
Hub Cloud Security Posture Management (CSPM) controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub::standards/cis-aws-foundations-benchmark/
v/1.4.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
    "ControlId": "3.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",

```



```

    "Region": "us-east-1"
  },
],
"Compliance": {
  "Status": "FAILED",
  "RelatedRequirements": [
    "CIS AWS Foundations Benchmark v1.4.0/3.7"
  ],
  "SecurityControlId": "CloudTrail.2",
  "AssociatedStandards": [{
    "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
  }]
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS Foundations Benchmark"
  ]
}
}

```

Ejemplo de hallazgo para CIS AWS Foundations Benchmark v1.2.0

El siguiente ejemplo proporciona un ejemplo de la búsqueda de un control que se aplica a CIS AWS Foundations Benchmark v1.2.0. En este ejemplo, los resultados del control consolidado están desactivados.

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",

```

```

"Region": "us-east-2",
"GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/
rule/2.7",
"AwsAccountId": "123456789012",
"Types": [
  "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
],
"FirstObservedAt": "2020-08-29T04:10:06.337Z",
"LastObservedAt": "2021-09-28T16:10:05.350Z",
"CreatedAt": "2020-08-29T04:10:06.337Z",
"UpdatedAt": "2021-09-28T16:10:00.087Z",
"Severity": {
  "Product": 40,
  "Label": "MEDIUM",
  "Normalized": 40,
  "Original": "MEDIUM"
},
"Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
"Description": "AWS Key Management Service (KMS) is a managed service that helps
create and control the encryption keys used to encrypt account data, and uses Hardware
Security Modules (HSMs) to protect the security of encryption keys. CloudTrail
logs can be configured to leverage server side encryption (SSE) and KMS customer
created master keys (CMK) to further protect CloudTrail logs. It is recommended that
CloudTrail be configured to use SSE-KMS.",
"Remediation": {
  "Recommendation": {
    "Text": "For directions on how to correct this issue, consult the AWS Security
Hub Cloud Security Posture Management (CSPM) controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsGuideArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0",
  "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
  "RuleId": "2.7",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
  "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
  "Related AWS Resources:0/type": "AWS::Config::ConfigRule",

```

```

    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-
foundations-benchmark/v/1.2.0/2.7",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    }
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
  ]
}

```

Ejemplo de hallazgo para la norma NIST SP 800-53, revisión 5

El siguiente ejemplo proporciona un ejemplo del hallazgo de un control que se aplica a la norma NIST SP 800-53, revisión 5. En este ejemplo, los resultados de los controles consolidados están desactivados.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2023-02-17T14:22:46.726Z",
  "LastObservedAt": "2023-02-17T14:22:50.846Z",
  "CreatedAt": "2023-02-17T14:22:46.726Z",
  "UpdatedAt": "2023-02-17T14:22:46.726Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to fix this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) NIST 800-53 R5 documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-53/v/5.0.0",

```

```

    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-53/v/5.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/
v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",

      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",

      "Partition": "aws",

      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "NIST.800-53.r5 AU-9",
      "NIST.800-53.r5 CA-9(1)",
      "NIST.800-53.r5 CM-3(6)",
      "NIST.800-53.r5 SC-13",
      "NIST.800-53.r5 SC-28",
      "NIST.800-53.r5 SC-28(1)",
      "NIST.800-53.r5 SC-7(10)",
      "NIST.800-53.r5 SI-7(6)"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [

```

```

    {
      "StandardsId": "standards/nist-800-53/v/5.0.0"
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2023-02-17T14:22:53.572Z"
}

```

Ejemplo de hallazgo de la norma NIST SP 800-171, revisión 2

El siguiente ejemplo proporciona un ejemplo del hallazgo de un control que se aplica a la norma NIST SP 800-171, revisión 2. En este ejemplo, los resultados de los controles consolidados están desactivados.

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/v/2.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-171/v/2.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "AwsAccountName": "TestAcct",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2025-05-29T05:23:58.690Z",

```

```

"LastObservedAt": "2025-05-30T05:50:11.898Z",
"CreatedAt": "2025-05-29T05:24:24.772Z",
"UpdatedAt": "2025-05-30T05:50:34.292Z",
"Severity": {
  "Product": 40,
  "Label": "MEDIUM",
  "Normalized": 40,
  "Original": "MEDIUM"
},
"Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
"Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
"Remediation": {
  "Recommendation": {
    "Text": "For information on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/nist-800-171/v/2.0.0",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/v/2.0.0",
  "ControlId": "CloudTrail.2",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation",
  "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-0ab1c2d4",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/nist-800-171/v/2.0.0/CloudTrail.2",
  "aws/securityhub/ProductName": "Security Hub",
  "aws/securityhub/CompanyName": "AWS",
  "Resources:0/Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-BaselineCloudTrail",
  "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/v/2.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
},
"Resources": [
  {
    "Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-BaselineCloudTrail",

```

```

    "Partition": "aws",
    "Region": "us-east-1",
    "Type": "AwsCloudTrailTrail"
  }
],
"Compliance": {
  "Status": "FAILED",
  "SecurityControlId": "CloudTrail.2",
  "RelatedRequirements": [
    "NIST.800-171.r2/3.3.8"
  ],
  "AssociatedStandards": [
    {
      "StandardsId": "standards/nist-800-171/v/2.0.0"
    }
  ]
},
"Workflow": {
  "Status": "NEW"
},
"WorkflowState": "NEW",
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  }
},
"ProcessedAt": "2025-05-30T05:50:40.297Z"
}

```

Ejemplo de búsqueda del estándar de seguridad de datos de la industria de tarjetas de pago, versión 3.2.1

En el siguiente ejemplo, se proporciona un ejemplo de la búsqueda de un control que se aplica a la norma de seguridad de datos del sector de las tarjetas de pago (PCI DSS), versión 3.2.1. En este ejemplo, los resultados de control consolidados están deshabilitados.


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.089Z",
  "LastObservedAt": "2021-09-28T16:10:06.942Z",
  "CreatedAt": "2020-08-06T02:18:23.089Z",
  "UpdatedAt": "2021-09-28T16:10:00.090Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest using AWS KMS CMKs",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption by checking if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1",
    "ControlId": "PCI.CloudTrail.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation",
  }
}
```

```

    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "PCI DSS 3.4"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/pci-dss/v/3.2.1"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    }
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ]
}

```

```

    ]
  }
}

```

Ejemplo de hallazgo para el estándar AWS de etiquetado de recursos

En el siguiente ejemplo, se proporciona un ejemplo de la búsqueda de un control que se aplica al estándar de etiquetado AWS de recursos. En este ejemplo, los resultados del control consolidado están deshabilitados.

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "security-control/EC2.44",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-02-19T21:00:32.206Z",
  "LastObservedAt": "2024-04-29T13:01:57.861Z",
  "CreatedAt": "2024-02-19T21:00:32.206Z",
  "UpdatedAt": "2024-04-29T13:01:41.242Z",
  "Severity": {
    "Label": "LOW",
    "Normalized": 1,
    "Original": "LOW"
  },
  "Title": "EC2 subnets should be tagged",
  "Description": "This control checks whether an Amazon EC2 subnet has tags with the specific keys defined in the parameter requiredTagKeys. The control fails if the subnet doesn't have any tag keys or if it doesn't have all the keys specified in the parameter requiredTagKeys. If the parameter requiredTagKeys isn't provided, the control only checks for the existence of a tag key and fails if the subnet isn't tagged with any key. System tags, which are automatically applied and begin with aws:, are ignored.",
  "Remediation": {
    "Recommendation": {

```

```

    "Text": "For information on how to correct this issue, consult the AWS Security
Hub Cloud Security Posture Management (CSPM) controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.44/remediation"
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-tagged-ec2-subnet-6ceafede",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "No tags are present.",
    "Resources:0/Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
securityhub/arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsEc2Subnet",
      "Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/subnet-1234567890abcdef0",
      "Partition": "aws",
      "Region": "eu-central-1",
      "Details": {
        "AwsEc2Subnet": {
          "AssignIpv6AddressOnCreation": false,
          "AvailabilityZone": "eu-central-1b",
          "AvailabilityZoneId": "euc1-az3",
          "AvailableIpAddressCount": 4091,
          "CidrBlock": "10.24.34.0/23",
          "DefaultForAz": true,
          "MapPublicIpOnLaunch": true,
          "OwnerId": "123456789012",
          "State": "available",
          "SubnetArn": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
          "SubnetId": "subnet-1234567890abcdef0",
          "VpcId": "vpc-021345abcdef6789"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",

```

```

    "SecurityControlId": "EC2.44",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/aws-resource-tagging-standard/v/1.0.0"
      }
    ],
    "SecurityControlParameters": [
      {
        "Name": "requiredTagKeys",
        "Value": [
          "peepoo"
        ]
      }
    ],
    },
    "WorkflowState": "NEW",
    "Workflow": {
      "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
      "Severity": {
        "Label": "LOW",
        "Original": "LOW"
      },
      "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards"
      ]
    },
    "ProcessedAt": "2024-04-29T13:02:03.259Z"
  }
}

```

Ejemplo de hallazgo para el estándar de AWS Control Tower gestión de servicios

En el siguiente ejemplo, se proporciona un ejemplo de la búsqueda de un control que se aplica al estándar de administración de AWS Control Tower servicios. En este ejemplo, los resultados del control consolidado están deshabilitados.

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",

```

```

"ProductName": "Security Hub CSPM",
"CompanyName": "AWS",
"Region": "us-east-1",
"GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
"AwsAccountId": "123456789012",
"Types": [
  "Software and Configuration Checks/Industry and Regulatory Standards"
],
"FirstObservedAt": "2022-11-17T01:25:30.296Z",
"LastObservedAt": "2022-11-17T01:25:45.805Z",
"CreatedAt": "2022-11-17T01:25:30.296Z",
"UpdatedAt": "2022-11-17T01:25:30.296Z",
"Severity": {
  "Product": 40,
  "Label": "MEDIUM",
  "Normalized": 40,
  "Original": "MEDIUM"
},
"Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",
"Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
"Remediation": {
  "Recommendation": {
    "Text": "For information on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/service-managed-aws-control-tower/v/1.0.0",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
  "ControlId": "CT.CloudTrail.2",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation",
  "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-fe95bf3f",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "aws/securityhub/ProductName": "Security Hub CSPM",
  "aws/securityhub/CompanyName": "AWS",

```

```

    "Resources/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-
aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS:::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}

```

Ejemplo de hallazgo consolidado para varios estándares

El siguiente ejemplo proporciona un ejemplo de la búsqueda de un control que se aplica a varios estándares habilitados. En este ejemplo, se habilitan las conclusiones de control consolidadas.

```
{
```

```

"SchemaVersion": "2018-10-08",
"Id": "arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
"ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
"ProductName": "Security Hub",
"CompanyName": "AWS",
"Region": "us-east-1",
"GeneratorId": "security-control/CloudTrail.2",
"AwsAccountId": "123456789012",
"Types": [
  "Software and Configuration Checks/Industry and Regulatory Standards"
],
"FirstObservedAt": "2024-08-09T14:57:04.521Z",
"LastObservedAt": "2025-05-30T03:30:17.407Z",
"CreatedAt": "2024-08-09T14:57:04.521Z",
"UpdatedAt": "2025-05-30T03:30:32.781Z",
"Severity": {
  "Label": "MEDIUM",
  "Normalized": 40,
  "Original": "MEDIUM"
},
"Title": "CloudTrail should have encryption at-rest enabled",
"Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
"Remediation": {
  "Recommendation": {
    "Text": "For information on how to correct this issue, consult the AWS Security Hub Cloud Security Posture Management (CSPM) controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-01a2b345",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "aws/securityhub/ProductName": "Security Hub",
  "aws/securityhub/CompanyName": "AWS",
  "Resources:0/Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-D0-NOT-DELETE",
  "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
},

```



```

"Resources": [
  {
    "Type": "AwsCloudTrailTrail",
    "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-DO-NOT-DELETE",
    "Partition": "aws",
    "Region": "us-east-1",
    "Details": {
      "AwsCloudTrailTrail": {
        "HasCustomEventSelectors": false,
        "IncludeGlobalServiceEvents": true,
        "LogFileValidationEnabled": true,
        "HomeRegion": "us-east-1",
        "IsMultiRegionTrail": true,
        "S3BucketName": "cloudtrail-awslogs-do-not-delete",
        "IsOrganizationTrail": false,
        "Name": "TestTrail-DO-NOT-DELETE"
      }
    }
  }
],
"Compliance": {
  "Status": "FAILED",
  "SecurityControlId": "CloudTrail.2",
  "RelatedRequirements": [
    "CIS AWS Foundations Benchmark v1.2.0/2.7",
    "CIS AWS Foundations Benchmark v1.4.0/3.7",
    "CIS AWS Foundations Benchmark v3.0.0/3.5",
    "NIST.800-171.r2/3.3.8",
    "PCI DSS v3.2.1/3.4",
    "PCI DSS v4.0.1/10.3.2"
  ],
  "AssociatedStandards": [
    { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
    { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
    { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
    { "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"},
    { "StandardsId": "standards/nist-800-171/v/2.0.0"},
    { "StandardsId": "standards/pci-dss/v/3.2.1"},
    { "StandardsId": "standards/pci-dss/v/4.0.1"}
  ]
},
"Workflow": {
  "Status": "NEW"
},

```

```
"WorkflowState": "NEW",
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "Severity": {
    "Normalized": 40,
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  }
},
"ProcessedAt": "2025-05-30T03:31:00.831Z"
}
```

Descripción de las integraciones en Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (CSPM) puede asimilar los hallazgos de seguridad de varias Servicios de AWS soluciones de seguridad de terceros AWS Partner Network compatibles. Estas integraciones pueden ayudarlo a obtener una visión integral de la seguridad y el cumplimiento en todo su entorno. AWS Security Hub CSPM ingiere los resultados de las soluciones integradas y los convierte al AWS Security Finding Format (ASFF).

Important

En el caso de las integraciones de productos compatibles AWS y de terceros, Security Hub CSPM recibe y consolida las conclusiones que se generan solo después de activar Security Hub CSPM para usted. Cuentas de AWS El servicio no recibe ni consolida retroactivamente las conclusiones de seguridad que se generaron antes de activar Security Hub CSPM.

La página de integraciones de la consola CSPM de Security Hub proporciona acceso a las integraciones de productos disponibles AWS y de terceros. La API CSPM de Security Hub también tiene operaciones para gestionar las integraciones.

Es posible que una integración no esté disponible en todas. Regiones de AWS Si una integración no es compatible en la región en la que ha iniciado sesión actualmente en la consola CSPM de Security Hub, no aparecerá en la página de integraciones de la consola. Para obtener una lista de las integraciones que están disponibles en las regiones de China y AWS GovCloud (US) Regions, consulte [Disponibilidad de las integraciones por región](#).

Además de las Servicio de AWS integraciones integradas de terceros, puede integrar productos de seguridad personalizados con Security Hub CSPM. Para obtener más información, consulte [Integración de Security Hub CSPM con productos personalizados](#).

Revisión de una lista de integraciones de Security Hub CSPM

Elige el método que prefieras y sigue los pasos para revisar una lista de integraciones en AWS Security Hub Cloud Security Posture Management (CSPM) o los detalles sobre una integración específica.

Security Hub CSPM console

Para revisar las opciones y los detalles de la integración (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en.
<https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación CSPM de Security Hub, elija Integraciones.

En la página Integraciones, aparecen primero las integraciones con otros, seguidas de Servicios de AWS las integraciones con productos de terceros.

Para cada integración, la página Integraciones proporciona la siguiente información:

- El nombre de la empresa
- El nombre del producto
- Una descripción de la integración
- Las categorías a las que se aplica la integración
- Cómo habilitar la integración
- El estado actual de la integración

Puede filtrar la lista utilizando texto de los siguientes campos:

- Nombre de la empresa
- Nombre del producto
- Descripción de integración
- Categorías

Security Hub CSPM API

Para revisar las opciones y los detalles de la integración (API)

Para obtener una lista de integraciones, utilice la operación [DescribeProducts](#). Si está utilizando el AWS CLI, ejecute el [describe-products](#) comando.

Para recuperar los detalles de una integración de productos específica, utilice el ProductArn parámetro para especificar el nombre de recurso de Amazon (ARN) de la integración.

Por ejemplo, el siguiente AWS CLI comando recupera detalles sobre la integración de Security Hub CSPM con 3. CORESec

```
$ aws securityhub describe-products --product-arn "arn:aws:securityhub:us-east-1::product/3coresec/3coresec"
```

Habilitar el flujo de hallazgos desde una integración de Security Hub (CSPM)

En la página de integraciones de la consola AWS Security Hub Cloud Security Posture Management (CSPM), puede ver los pasos necesarios para habilitar cada integración.

Para la mayoría de las integraciones con otros Servicios de AWS, el único paso necesario para habilitar la integración es habilitar el otro servicio. La información de integración incluye un enlace a la página principal del otro servicio. Al habilitar el otro servicio, se crea y aplica automáticamente un permiso a nivel de recurso que permite a Security Hub CSPM recibir las conclusiones del servicio.

En el caso de las integraciones de productos de terceros, es posible que tenga que comprar la integración en el y AWS Marketplace, a continuación, configurarla. La información de integración proporciona enlaces para completar estas tareas.

Si hay más de una versión de un producto disponible AWS Marketplace, selecciona la versión a la que deseas suscribirte y, a continuación, selecciona Continuar con la suscripción. Por ejemplo, algunos productos ofrecen una versión estándar y una AWS GovCloud (US) versión.

Cuando se habilita una integración de productos, se asocia automáticamente una política de recursos a la suscripción del producto. Esta política de recursos define los permisos que Security Hub CSPM necesita para recibir las conclusiones de ese producto.

Una vez que haya completado los pasos preliminares para habilitar una integración, puede deshabilitar y volver a habilitar el flujo de resultados desde esa integración. En la página Integraciones, para las integraciones que envíen resultados, el campo Estado indica si está actualmente aceptando resultados.

Security Hub CSPM console

Para deshabilitar y habilitar el flujo de resultados desde una integración (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación CSPM de Security Hub, elija Integraciones.
3. En el caso de las integraciones que envían conclusiones, la información de estado indica si Security Hub CSPM acepta actualmente las conclusiones de esa integración.
4. Seleccione Aceptar los resultados.

Security Hub CSPM API

Utilice la operación [EnableImportFindingsForProduct](#). Si está utilizando el AWS CLI, ejecute el comando. [enable-import-findings-for-product](#) Para permitir que Security Hub reciba resultados desde una integración, necesita el ARN del producto. Para obtener las ARNs integraciones disponibles, utilice la [DescribeProducts](#) operación. Si está utilizando el AWS CLI, ejecute el [describe-products](#).

Por ejemplo, el siguiente AWS CLI comando permite que Security Hub CSPM reciba las conclusiones de la integración de CrowdStrike Falcon. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub enable-import-findings-for product --product-arn  
"arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

Deshabilitar el flujo de hallazgos de una integración de Security Hub (CSPM)

Elige el método que prefieras y sigue los pasos para deshabilitar el flujo de hallazgos de una integración de AWS Security Hub Cloud Security Posture Management (CSPM).

Security Hub CSPM console

Para deshabilitar el flujo de resultados desde una integración (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación CSPM de Security Hub, elija Integraciones.
3. En el caso de las integraciones que envían conclusiones, la información de estado indica si Security Hub CSPM acepta actualmente las conclusiones de esa integración.
4. Seleccione Dejar de aceptar resultados.

Security Hub CSPM API

Utilice la operación [DisableImportFindingsForProduct](#). Si está utilizando el AWS CLI, ejecute el comando [disable-import-findings-for-product](#). Para desactivar el flujo de resultados de una integración, necesita el ARN de suscripción para la integración habilitada. Para obtener el ARN de suscripción, utilice la operación [ListEnabledProductsForImport](#). Si está utilizando el AWS CLI, ejecute el [list-enabled-products-for-import](#).

Por ejemplo, el siguiente AWS CLI comando deshabilita el flujo de hallazgos hacia Security Hub CSPM desde la CrowdStrike integración de Falcon. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub disable-import-findings-for-product --product-subscription-arn  
"arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/  
crowdstrike-falcon"
```

Visualización de los resultados de una integración de Security Hub (CSPM)

Al empezar a aceptar las conclusiones de una integración de AWS Security Hub Cloud Security Posture Management (CSPM), la página Integraciones de la consola CSPM de Security Hub muestra el estado de la integración como Aceptando las conclusiones. Para revisar una lista de las conclusiones de la integración, seleccione Ver las conclusiones.

La lista de resultados muestra los resultados activos de la integración seleccionada que tienen un estado de flujo de trabajo NEW o NOTIFIED.

Si habilita la agregación entre regiones, en la región de agregación, la lista incluye los resultados de la región de agregación y de las regiones vinculadas en las que la integración esté habilitada. Security Hub no habilita de forma automática las integraciones basadas en la configuración de agregación entre regiones.

En otras regiones, la lista de resultados de una integración solo contiene los resultados de la región actual.

Para obtener información sobre cómo configurar la agregación entre regiones, consulte [Agregación de datos del CSPM en todas las regiones](#).

En la lista de resultados puede realizar las siguientes acciones.

- [Cambiar los filtros y la agrupación de la lista](#)
- [Ver los detalles de cada resultado](#)
- [Actualizar el estado de flujo de trabajo de los resultados](#)
- [Enviar los resultados a acciones personalizadas](#)

Servicio de AWS integraciones con Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (CSPM) admite integraciones con varios otros. Servicios de AWS

Note

Es posible que las integraciones no estén disponibles en todas. Regiones de AWS Si en la región actual no se admite una integración, esta no aparece en la página Integraciones. Para obtener una lista de las integraciones que están disponibles en las regiones de China y AWS GovCloud (US), consulte [the section called “Integraciones compatibles en las regiones de China \(Pekín\) y China \(Ningxia\)” y the section called “Integraciones compatibles en las regiones \(EE. UU. este\) y AWS GovCloud AWS GovCloud \(EE. UU., oeste\)”](#).

A menos que se indique a continuación, Servicio de AWS las integraciones que envían los resultados a Security Hub CSPM se activan automáticamente después de activar Security Hub CSPM y el otro

servicio. Las integraciones que reciben los resultados del CSPM de Security Hub pueden requerir pasos adicionales para su activación. Revise la información sobre cada integración para obtener más información.

Descripción general de las integraciones de AWS servicios con Security Hub (CSPM)

Esta es una descripción general de AWS los servicios que envían las conclusiones al Security Hub CSPM o reciben las conclusiones del Security Hub CSPM.

Servicio integrado AWS	Dirección	
AWS Config	Envía resultados	
AWS Firewall Manager	Envía resultados	
Amazon GuardDuty	Envía resultados	
AWS Health	Envía resultados	
AWS Identity and Access Management Access Analyzer	Envía resultados	
Amazon Inspector	Envía resultados	
AWS IoT Device Defender	Envía resultados	
Amazon Macie	Envía resultados	
AWS Systems Manager Patch Manager	Envía resultados	
AWS Audit Manager	Recibe resultados	
Amazon Q Developer en aplicaciones de chat	Recibe resultados	
Amazon Detective	Recibe resultados	
Amazon Security Lake	Recibe resultados	

Servicio integrado AWS	Dirección	
AWS Systems Manager Explorer y OpsCenter	Recibe y actualiza resultados	
AWS Trusted Advisor	Recibe resultados	

AWS servicios que envían los resultados a Security Hub (CSPM)

Los siguientes AWS servicios se integran con el Security Hub CSPM mediante el envío de las conclusiones al Security Hub CSPM. Security Hub CSPM convierte los hallazgos al formato [AWS Security Finding](#).

AWS Config (Envía los resultados)

AWS Config es un servicio que le permite evaluar, auditar y evaluar las configuraciones de sus AWS recursos. AWS Config supervisa y registra continuamente las configuraciones de sus AWS recursos y le permite automatizar la evaluación de las configuraciones registradas comparándolas con las configuraciones deseadas.

Al utilizar la integración con AWS Config, puede ver los resultados de las evaluaciones de reglas AWS Config gestionadas y personalizadas como hallazgos en Security Hub CSPM. Estos hallazgos se pueden ver junto con otros hallazgos del CSPM de Security Hub, lo que proporciona una visión general completa de su postura de seguridad.

AWS Config utiliza Amazon EventBridge para enviar las evaluaciones de las AWS Config reglas a Security Hub (CSPM). Security Hub CSPM transforma las evaluaciones de las reglas en hallazgos que siguen el formato de [búsqueda AWS de seguridad](#). Luego, Security Hub CSPM enriquece los hallazgos haciendo todo lo posible al obtener más información sobre los recursos afectados, como el nombre del recurso de Amazon (ARN), las etiquetas de los recursos y la fecha de creación.

Para obtener más información sobre esta integración, consulte las secciones siguientes.

Cómo AWS Config envía los resultados a Security Hub (CSPM)

Todos los resultados de Security Hub CSPM utilizan el formato JSON estándar de ASFF. El ASFF incluye detalles sobre el origen del hallazgo, el recurso afectado y el estado actual del hallazgo. AWS Config envía evaluaciones de reglas gestionadas y personalizadas a Security Hub CSPM a través

de. EventBridge Security Hub CSPM transforma las evaluaciones de las reglas en conclusiones que siguen la ASFF y enriquece las conclusiones haciendo todo lo posible.

Tipos de hallazgos que se AWS Config envían a Security Hub (CSPM)

Una vez activada la integración, AWS Config envía las evaluaciones de todas las reglas AWS Config administradas y las reglas personalizadas a Security Hub CSPM. Solo se envían las evaluaciones que se realizaron después de habilitar el CSPM de Security Hub. Por ejemplo, supongamos que la evaluación de una AWS Config regla revela cinco recursos fallidos. Si activo el CSPM de Security Hub después de eso y la regla revela un sexto recurso fallido, solo se AWS Config envía la evaluación del sexto recurso al Security Hub CSPM.

Se excluyen las evaluaciones de [AWS Config las reglas vinculadas a servicios](#), como las que se utilizan para ejecutar comprobaciones en los controles CSPM de Security Hub.

Envío de AWS Config los resultados a Security Hub (CSPM)

Cuando se active la integración, el Security Hub CSPM asignará automáticamente los permisos necesarios para recibir las conclusiones. AWS Config Security Hub CSPM utiliza permisos de service-to-service nivel que le proporcionan una forma segura de activar esta integración e importar los resultados desde AWS Config Amazon. EventBridge

Latencia para el envío de resultados

Cuando AWS Config crea un nuevo hallazgo, normalmente puede verlo en Security Hub CSPM en cinco minutos.

Reintentarlo cuando el CSPM de Security Hub no está disponible

AWS Config envía las conclusiones al Security Hub CSPM haciendo todo lo posible. EventBridge Cuando un evento no se entrega correctamente a Security Hub CSPM, EventBridge vuelve a intentar la entrega hasta 24 horas o 185 veces, lo que ocurra primero.

Actualización de los AWS Config hallazgos existentes en Security Hub (CSPM)

Tras AWS Config enviar un hallazgo al Security Hub CSPM, este puede enviar actualizaciones del mismo hallazgo al Security Hub CSPM para reflejar observaciones adicionales de la actividad de búsqueda. Las actualizaciones solo se envían para eventos de `ComplianceChangeNotification`. Si no se produce ningún cambio de conformidad, las actualizaciones no se envían a Security Hub CSPM. Security Hub CSPM elimina los resultados 90 días después de la actualización más reciente o 90 días después de su creación si no se produce ninguna actualización.

Security Hub CSPM no archiva las conclusiones que se envían AWS Config incluso si se elimina el recurso asociado.

Regiones en las que existen hallazgos AWS Config

AWS Config los hallazgos se producen a nivel regional. AWS Config envía las conclusiones al Security Hub (CSPM) de la misma región o regiones en las que se producen las conclusiones.

Visualización de AWS Config los resultados en Security Hub (CSPM)

Para ver sus AWS Config hallazgos, elija Hallazgos en el panel de navegación CSPM de Security Hub. Para filtrar los resultados y mostrar solo los AWS Config hallazgos, elija el nombre del producto en el menú desplegable de la barra de búsqueda. Introduzca Config y seleccione Aplicar.

Interpretación y AWS Config búsqueda de nombres en Security Hub (CSPM)

Security Hub CSPM transforma las evaluaciones de las AWS Config reglas en hallazgos que siguen las [AWS Formato de búsqueda de seguridad \(ASFF\)](#) AWS Config las evaluaciones de reglas utilizan un patrón de eventos diferente al de la ASFF. La siguiente tabla mapea los campos de evaluación de AWS Config reglas con sus homólogos de ASFF tal como aparecen en Security Hub CSPM.

Configuración de tipo de resultado de la evaluación de reglas	Tipo de resultado ASFF	Valor codificado
detalle. awsAccountId	AwsAccountId	
detalle. newEvaluationResult. resultRecordedTime	CreatedAt	
detalle. newEvaluationResult. resultRecordedTime	UpdatedAt	
	ProductArn	<partition><region>«arn ::securityhub::»product/aws/config
	ProductName	"Config"
	CompanyName	"AWS"

Configuración de tipo de resultado de la evaluación de reglas	Tipo de resultado ASFF	Valor codificado
	Región	"eu-central-1"
configRuleArn	GeneratorId, ProductFields	
detalle. ConfigRuleARN/finding/hash	Id	
detalle. configRuleName	Título, ProductFields	
detalle. configRuleName	Descripción	"Este resultado se crea para un cambio de conformidad del recurso para la regla de configuración: \${detalle. ConfigRuleName} "
Elemento de configuración «ARN» o ARN computado por CSPM de Security Hub	Resources[i].id	
detail.resourceType	Resources[i].Type	"AwsS3Bucket"
	Resources[i].Partition	"aws"
	Resources[i].Region	"eu-central-1"
Elemento de configuración "configuración"	Resources[i].Details	
	SchemaVersion	"10/08/2018"
	Severity.Label	Consultar "Interpretación de la etiqueta de gravedad" a continuación
	Tipos	["Comprobaciones de configuración y software"]

Configuración de tipo de resultado de la evaluación de reglas	Tipo de resultado ASFF	Valor codificado
detalle. newEvaluationResult. Tipo de conformidad	Compliance.Status	“NO_APROBADO”, “NO_DISPONIBLE”, “APROBADO” o “ADVERTENCIA”
	Workflow.Status	«RESUELTO» si se genera una AWS Config constatación con un estado de conformidad de «APROBADO» o si el estado de conformidad cambia de «FALLIDO» a «APROBADO». De lo contrario, Workflow.Status será “NUEVO”. Puedes cambiar este valor con la operación de la API. BatchUpdateFindings

Interpretación de la etiqueta de gravedad

Todos los resultados de las evaluaciones de las AWS Config reglas tienen una etiqueta de gravedad predeterminada de MEDIUM en el ASFF. Puede actualizar la etiqueta de gravedad de un resultado con la operación de la API [BatchUpdateFindings](#).

Hallazgo típico de AWS Config

Security Hub CSPM transforma las evaluaciones de AWS Config reglas en hallazgos que siguen la ASFF. El siguiente es un ejemplo de un hallazgo típico del ASFF AWS Config .

Note

Si la descripción contiene más de 1024 caracteres, se truncará en 1024 caracteres y al final dirá “(truncada)”.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/finding/45g070df80cb50b68fa6a43594kc6fda1e517932",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/config",
  "ProductName": "Config",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks"
  ],
  "CreatedAt": "2022-04-15T05:00:37.181Z",
  "UpdatedAt": "2022-04-19T21:20:15.056Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "s3-bucket-level-public-access-prohibited-config-integration-demo",
  "Description": "This finding is created for a resource compliance change for config rule: s3-bucket-level-public-access-prohibited-config-integration-demo",
  "ProductFields": {
    "aws/securityhub/ProductName": "Config",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/config/arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/finding/46f070df80cd50b68fa6a43594dc5fda1e517902",
    "aws/config/ConfigRuleArn": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq",
    "aws/config/ConfigRuleName": "s3-bucket-level-public-access-prohibited-config-integration-demo",
    "aws/config/ConfigComplianceType": "NON_COMPLIANT"
  },
  "Resources": [{
    "Type": "AwsS3Bucket",
    "Id": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Partition": "aws",
    "Region": "eu-central-1",
    "Details": {
      "AwsS3Bucket": {
        "OwnerId": "4edbbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
```

```
    "CreatedAt": "2022-04-15T04:32:53.000Z"
  }
}
]],
"Compliance": {
  "Status": "FAILED"
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "MEDIUM"
  },
  "Types": [
    "Software and Configuration Checks"
  ]
}
}
```

Habilitación y configuración de la integración

Tras activar Security Hub CSPM, esta integración se activa automáticamente. AWS Config comienza inmediatamente a enviar los resultados al Security Hub CSPM.

Detener la publicación de los hallazgos en Security Hub (CSPM)

Para dejar de enviar los resultados a Security Hub CSPM, puede utilizar la consola CSPM de Security Hub o la API CSPM de Security Hub.

Para obtener instrucciones sobre cómo detener el flujo de resultados, consulte [Habilitar el flujo de hallazgos desde una integración de Security Hub \(CSPM\)](#).

AWS Firewall Manager (Envía los resultados)

Firewall Manager envía los resultados al Security Hub CSPM cuando una política de firewall de aplicaciones web (WAF) para los recursos o una regla de lista de control de acceso web (ACL web) no cumple con los requisitos. Firewall Manager también envía los resultados cuando AWS Shield Advanced no protege los recursos o cuando se identifica un ataque.

Tras activar Security Hub CSPM, esta integración se activa automáticamente. Firewall Manager comienza inmediatamente a enviar los resultados al Security Hub CSPM.

Para obtener más información sobre la integración, consulte la página de integraciones de la consola CSPM de Security Hub.

Para obtener más información sobre Firewall Manager, consulte la [Guía para desarrolladores de AWS WAF](#).

Amazon GuardDuty (envía los resultados)

GuardDuty envía todos los tipos de hallazgos que genera al Security Hub CSPM. Algunos tipos de búsqueda tienen requisitos previos, requisitos de habilitación o limitaciones regionales. Para obtener más información, consulta la [GuardDuty búsqueda de tipos](#) en la Guía del GuardDuty usuario de Amazon.

Los nuevos hallazgos GuardDuty se envían al Security Hub CSPM en cinco minutos. Las actualizaciones de los resultados se envían en función de la configuración de resultados actualizados de Amazon EventBridge en GuardDuty la configuración.

Al generar resultados de GuardDuty muestra mediante la página de GuardDuty configuración, Security Hub CSPM recibe los resultados de muestra y omite el prefijo [Sample] en el tipo de hallazgo. Por ejemplo, el ejemplo del tipo de búsqueda GuardDuty [SAMPLE] Recon:IAMUser/ResourcePermissions se muestra como Recon:IAMUser/ResourcePermissions en Security Hub CSPM.

Tras activar Security Hub CSPM, esta integración se activa automáticamente. GuardDuty comienza inmediatamente a enviar los resultados al Security Hub CSPM.

Para obtener más información sobre la GuardDuty integración, consulte [Integración con AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) en la Guía GuardDuty del usuario de Amazon.

AWS Health (Envía los resultados)

AWS Health proporciona una visibilidad continua del rendimiento de sus recursos y de la disponibilidad de sus Servicios de AWS y Cuentas de AWS. Puede usar los eventos AWS Health para saber cómo pueden afectar los cambios de servicios y recursos a las aplicaciones que ejecuta en AWS.

La integración con AWS Health no utiliza `BatchImportFindings`. En su lugar, AWS Health utiliza la mensajería de service-to-service eventos para enviar las conclusiones al Security Hub (CSPM).

Para obtener más información sobre la integración, consulte las siguientes secciones.

Cómo AWS Health envía los resultados a Security Hub (CSPM)

En Security Hub CSPM, los problemas de seguridad se rastrean como hallazgos. Algunos hallazgos provienen de problemas detectados por otros AWS servicios o por socios externos. Security Hub CSPM también tiene un conjunto de reglas que utiliza para detectar problemas de seguridad y generar hallazgos.

Security Hub CSPM proporciona herramientas para gestionar los hallazgos de todas estas fuentes. Puede ver y filtrar listas de resultados y ver los detalles de una búsqueda. Consulte [Revisión de los detalles y el historial de búsquedas en Security Hub \(CSPM\)](#). También puede realizar un seguimiento del estado de una investigación sobre un resultado. Consulte [Configuración del estado del flujo de trabajo de los hallazgos en Security Hub \(CSPM\)](#).

Todos los hallazgos en Security Hub CSPM utilizan un formato JSON estándar denominado [AWS Formato de búsqueda de seguridad \(ASFF\)](#). ASFF incluye detalles sobre el origen del problema, los recursos afectados y el estado actual del resultado.

AWS Health es uno de los AWS servicios que envía los resultados a Security Hub CSPM.

Tipos de hallazgos que se AWS Health envían a Security Hub (CSPM)

Una vez habilitada la integración, AWS Health envía los resultados que cumplen con una o más de las especificaciones enumeradas a Security Hub CSPM. Security Hub CSPM ingiere los hallazgos del [AWS Formato de búsqueda de seguridad \(ASFF\)](#)

- Hallazgos que contienen alguno de los siguientes valores para: Servicio de AWS
 - RISK
 - ABUSE
 - ACM
 - CLOUDHSM
 - CLOUDTRAIL
 - CONFIG
 - CONTROLTOWER
 - DETECTIVE

- EVENTS
- GUARDDUTY
- IAM
- INSPECTOR
- KMS
- MACIE
- SES
- SECURITYHUB
- SHIELD
- SSO
- COGNITO
- IOTDEVICEDEFENDER
- NETWORKFIREWALL
- ROUTE53
- WAF
- FIREWALLMANAGER
- SECRETSMANAGER
- BACKUP
- AUDITMANAGER
- ARTIFACT
- CLOUDENDURE
- CODEGURU
- ORGANIZATIONS
- DIRECTORYSERVICE
- RESOURCEMANAGER
- CLOUDWATCH
- DRS
- INSPECTOR2
- RESILIENCEHUB

- Hallazgos con las palabras `securityabuse`, o `certificate` en el AWS Health `typeCode` campo
- Averigua dónde se encuentra el AWS Health servicio `risk` o `abuse`

Envío de AWS Health los resultados a Security Hub (CSPM)

Si decide aceptar las conclusiones de AWS Health, Security Hub CSPM asignará automáticamente los permisos necesarios para recibir las conclusiones. AWS Health Security Hub CSPM utiliza permisos de `service-to-service` nivel que le proporcionan una forma fácil y segura de habilitar esta integración e importar las conclusiones desde AWS Health Amazon EventBridge en su nombre. Al elegir `Accept Findings`, se otorga a Security Hub CSPM permiso para consumir los hallazgos de AWS Health

Latencia para el envío de resultados

Cuando AWS Health crea un nuevo hallazgo, normalmente se envía al Security Hub CSPM en un plazo de cinco minutos.

Reintentarlo cuando el CSPM de Security Hub no está disponible

AWS Health envía las conclusiones al Security Hub CSPM haciendo todo lo posible. EventBridge Cuando un evento no se entrega correctamente a Security Hub CSPM, EventBridge vuelve a intentar enviar el evento durante 24 horas.

Actualización de los hallazgos existentes en Security Hub (CSPM)

Tras AWS Health enviar un hallazgo al Security Hub CSPM, este puede enviar actualizaciones del mismo hallazgo para reflejar observaciones adicionales de la actividad de búsqueda al Security Hub CSPM.

Regiones en las que existen resultados

Para eventos globales, AWS Health envía los resultados al Security Hub CSPM en `us-east-1` (partición AWS), `cn-northwest-1` (partición de China) y `-1` (partición). `gov-us-west` GovCloud AWS Health envía los eventos específicos de la región al Security Hub (CSPM) de la misma región o regiones en las que se producen los eventos.

Visualización de AWS Health los resultados en Security Hub (CSPM)

Para ver sus AWS Health hallazgos en Security Hub CSPM, elija Findings en el panel de navegación. Para filtrar los hallazgos y mostrar solo AWS Health los hallazgos, selecciona Salud en el campo Nombre del producto.

Interpretación y AWS Health búsqueda de nombres en Security Hub (CSPM)

AWS Health envía los resultados al Security Hub CSPM mediante. [AWS Formato de búsqueda de seguridad \(ASFF\)](#) AWS Health la búsqueda utiliza un patrón de eventos diferente al del formato ASFF CSPM de Security Hub. La siguiente tabla detalla todos los campos de AWS Health búsqueda con su homólogo ASFF tal como aparecen en Security Hub CSPM.

Tipo de resultado de Estado	Tipo de resultado ASFF	Valor codificado
inscrita	AwsAccountId	
detail.startTime	CreatedAt	
detail.eventDescription.lastDescription	Descripción	
detalle. eventTypeCode	GeneratorId	
detail.eventArn (incluido account) + hash de detail.startTime	Id	
<region>«arn:aws:securityhub:::» product/aws/health	ProductArn	
account o resourceId	Resources[i].id	
	Resources[i].Type	“Otros”
	SchemaVersion	“10/08/2018”
	Severity.Label	Consultar “Interpretación de la etiqueta de gravedad” a continuación

Tipo de resultado de Estado	Tipo de resultado ASFF	Valor codificado
«-» detalle.AWS Health eventTypeCode	Título	
-	Tipos	["Comprobaciones de configuración y software"]
event.time	UpdatedAt	
URL del evento de la consola Estado	SourceUrl	

Interpretación de la etiqueta de gravedad

La etiqueta de gravedad del resultado de ASFF se determina mediante la siguiente lógica:

- Gravedad CRÍTICA si:
 - El service campo del AWS Health hallazgo tiene el valor Risk
 - El typeCode campo del AWS Health hallazgo tiene el valor AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION
 - El typeCode campo del AWS Health hallazgo tiene el valor AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK
 - El typeCode campo del AWS Health hallazgo tiene el valor AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES

Gravedad ALTA si:

- El service campo del AWS Health hallazgo tiene el valor Abuse
- El typeCode campo del AWS Health hallazgo contiene el valor SECURITY_NOTIFICATION
- El typeCode campo del AWS Health hallazgo contiene el valor ABUSE_DETECTION

Gravedad MEDIA si:

- El campo service del resultado es cualquiera de los siguientes: ACM, ARTIFACT, AUDITMANAGER, BACKUP, CLOUDENDURE, CLOUDHSM, CLOUDTRAIL, CLOUDWATCH, CODEGURGU, COGNITO, CONFIG, CONTROLTOWER, DETECTIVE, DIRECTORYSERVICE, DRS, EVENTS, FIREWALLMANAGER, GUARDDUTY, IAM, INSPECTOR, INSPECTOR2,

IOTDEVICEDEFENDER, KMS, MACIE, NETWORKFIREWALL, ORGANIZATIONS, RESILIENCEHUB, RESOURCEMANAGER, ROUTE53, SECURITYHUB, SECRETSMANAGER, SES, SHIELD, SSO o WAF

- El campo typeCode del resultado AWS Health contiene el valor CERTIFICATE
- El campo typeCode del resultado AWS Health contiene el valor END_OF_SUPPORT

Hallazgo típico de AWS Health

AWS Health envía los resultados al Security Hub CSPM mediante. [AWS Formato de búsqueda de seguridad \(ASFF\)](#) A continuación se muestra un ejemplo de un hallazgo típico de AWS Health

Note

Si la descripción contiene más de 1024 caracteres, se truncará en 1024 caracteres y al final dirá (truncada).

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
  "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks"
  ],
  "CreatedAt": "2022-01-07T16:34:04.000Z",
  "UpdatedAt": "2022-01-07T19:17:43.000Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
  "Description": "Congratulations! Amazon SES has successfully detected the
MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\n\nYou can now use this MAIL
FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity
```

```

that is configured to use it. For information about how to configure a verified
identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/DeveloperGuide/mail-from-set.html .\\n\\nPlease note that this email only applies to
AWS Region US East (N. Virginia).",
    "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
    "ProductFields": {
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
        "aws/securityhub/ProductName": "Health",
        "aws/securityhub/CompanyName": "AWS"
    },
    "Resources": [
        {
            "Type": "Other",
            "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
        }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "MEDIUM"
        },
        "Types": [
            "Software and Configuration Checks"
        ]
    }
}
]
}

```

Habilitación y configuración de la integración

Tras activar Security Hub CSPM, esta integración se activa automáticamente. AWS Health comienza inmediatamente a enviar los resultados al Security Hub CSPM.

Detener la publicación de los hallazgos en Security Hub (CSPM)

Para dejar de enviar los resultados a Security Hub CSPM, puede utilizar la consola CSPM de Security Hub o la API CSPM de Security Hub.

Para obtener instrucciones sobre cómo detener el flujo de resultados, consulte [Habilitar el flujo de hallazgos desde una integración de Security Hub \(CSPM\)](#).

AWS Identity and Access Management Access Analyzer (Envía los resultados)

Con IAM Access Analyzer, todos los resultados se envían a Security Hub CSPM.

IAM Access Analyzer utiliza un razonamiento lógico para analizar las políticas basadas en recursos que se aplican a los recursos de la cuenta compatibles. IAM Access Analyzer genera un resultado cuando detecta una declaración de la política que permite que una entidad principal externa pueda acceder a un recurso de la cuenta.

En IAM Access Analyzer, solo la cuenta de administrador puede ver los resultados de los analizadores que se aplican a una organización. En el caso de los analizadores de la organización, el campo `AwsAccountId` ASFF refleja el ID de la cuenta de administrador. Bajo `ProductFields`, el campo `ResourceOwnerAccount` indica la cuenta en la que se descubrió el resultado. Si habilita los analizadores individualmente para cada cuenta, Security Hub CSPM genera varios resultados, uno que identifica el ID de la cuenta del administrador y otro que identifica el ID de la cuenta de recursos.

Para obtener más información, consulte [Integración con AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) en la Guía del usuario de IAM.

Amazon Inspector (Envía resultados)

Amazon Inspector es un servicio de gestión de vulnerabilidades que analiza continuamente sus cargas de trabajo en AWS en busca de vulnerabilidades. Amazon Inspector descubre y escanea automáticamente EC2 las instancias de Amazon y las imágenes de contenedores que se encuentran en Amazon Elastic Container Registry. El escaneo busca vulnerabilidades de software y exposición no deseada en la red.

Tras activar Security Hub CSPM, esta integración se activa automáticamente. Amazon Inspector comienza inmediatamente a enviar todas las conclusiones que genera a Security Hub (CSPM).

Para obtener más información sobre la integración, consulte [Integración con AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) en la Guía del usuario de Amazon Inspector.

Security Hub CSPM también puede recibir las conclusiones de Amazon Inspector Classic. Amazon Inspector Classic envía los resultados al Security Hub (CSPM) que se generan a través de las evaluaciones de todos los paquetes de reglas compatibles.

Para obtener más información sobre la integración, consulte [Integración con AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) en la Guía del usuario de Amazon Inspector Classic.

Los resultados de Amazon Inspector y Amazon Inspector Classic utilizan el mismo ARN de producto. Los resultados de Amazon Inspector presentan la siguiente entrada en ProductFields:

```
"aws/inspector/ProductVersion": "2",
```

AWS IoT Device Defender (Envía los resultados)

AWS IoT Device Defender es un servicio de seguridad que audita la configuración de sus dispositivos de IoT, monitorea los dispositivos conectados para detectar comportamientos anormales y ayuda a mitigar los riesgos de seguridad.

Tras activar AWS IoT Device Defender tanto el CSPM como el Security Hub, visita la [página de integraciones de la consola CSPM de Security Hub](#) y selecciona Aceptar los resultados para Auditar, Detectar o ambos. AWS IoT Device Defender Audit and Detect comienza a enviar todos los resultados al Security Hub (CSPM).

AWS IoT Device Defender La auditoría envía los resúmenes de las comprobaciones a Security Hub CSPM, que contienen información general sobre un tipo de comprobación de auditoría y una tarea de auditoría específicos. AWS IoT Device Defender Detect envía los hallazgos de infracciones relacionados con el aprendizaje automático (ML) y los comportamientos estadísticos y estáticos al Security Hub CSPM. La auditoría también envía las actualizaciones de búsqueda a Security Hub CSPM.

Para obtener más información sobre esta integración, consulte [Integración con AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) en la Guía para AWS IoT desarrolladores.

Amazon Macie (Envía resultados)

Un resultado de Macie puede indicar que existe una infracción potencial de la política o que hay información confidencial, como información de identificación personal (PII), presente en los datos que su organización almacena en Amazon S3.

Tras activar Security Hub CSPM, Macie comienza a enviar automáticamente las conclusiones de las políticas a Security Hub CSPM. Puede configurar la integración para que también envíe los hallazgos de datos confidenciales a Security Hub CSPM.

En Security Hub CSPM, el tipo de búsqueda de una política o de datos confidenciales se cambia a un valor compatible con ASFF. Por ejemplo, el tipo de `Policy:IAMUser/S3BucketPublic` búsqueda en Macie se muestra como `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic` en Security Hub CSPM.

Macie también envía los resultados de muestra generados a Security Hub CSPM. En el caso de los resultados de muestra, el nombre del recurso afectado es `macie-sample-finding-bucket` y el valor del campo `Sample` es `true`.

Para obtener más información, consulte la [integración de Amazon Macie con AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) en la Guía del usuario de Amazon Macie.

AWS Systems Manager Gestor de parches (envía los resultados)

AWS Systems Manager Patch Manager envía los resultados al Security Hub CSPM cuando las instancias de la flota de un cliente no cumplen con su estándar de cumplimiento de parches.

Patch Manager automatiza el proceso de aplicación de parches a instancias administradas con actualizaciones relacionadas con la seguridad y otros tipos de actualizaciones.

Tras activar Security Hub CSPM, esta integración se activa automáticamente. El administrador de parches de Systems Manager comienza inmediatamente a enviar los resultados al Security Hub (CSPM).

Para obtener más información acerca de cómo utilizar Patch Manager, consulte [AWS Systems Manager Patch Manager](#) en la Guía del usuario de AWS Systems Manager .

AWS servicios que reciben las conclusiones de Security Hub (CSPM)

Los siguientes AWS servicios están integrados con el Security Hub CSPM y reciben las conclusiones del Security Hub CSPM. Cuando se indique lo contrario, el servicio integrado también puede actualizar resultados. En este caso, la búsqueda de las actualizaciones que realice en el servicio integrado también se reflejará en Security Hub CSPM.

AWS Audit Manager (Recibe los resultados)

AWS Audit Manager recibe las conclusiones de Security Hub CSPM. Estos resultados ayudan a los usuarios de Audit Manager a prepararse para las auditorías.

Para obtener más información sobre Audit Manager, consulte la [Guía del usuario de AWS Audit Manager](#). AWS Las [comprobaciones de Security Hub Cloud Security Posture Management \(CSPM\) compatibles con AWS Audit Manager](#) las listas de controles para los que Security Hub CSPM envía las conclusiones a Audit Manager.

Desarrollador de Amazon Q en aplicaciones de chat (recibe las conclusiones)

Amazon Q Developer en aplicaciones de chat es un agente interactivo que te ayuda a supervisar e interactuar con tus AWS recursos en tus canales de Slack y salas de chat de Amazon Chime.

El desarrollador de aplicaciones de chat de Amazon Q recibe las conclusiones del CSPM de Security Hub.

Para obtener más información sobre la integración de Amazon Q Developer en aplicaciones de chat con Security Hub CSPM, consulte la descripción general de la [integración de CSPM de Security Hub en la Guía del administrador](#) de aplicaciones de chat para desarrolladores de Amazon Q.

Amazon Detective (Recibe resultados)

Detective recopila automáticamente los datos de registro de sus AWS recursos y utiliza el aprendizaje automático, el análisis estadístico y la teoría de grafos para ayudarlo a visualizar y llevar a cabo investigaciones de seguridad más rápidas y eficientes.

La integración de Security Hub CSPM con Detective le permite pasar de los GuardDuty hallazgos de Amazon en Security Hub CSPM a Detective. A continuación, puede utilizar las herramientas y visualizaciones de Detective para investigarlos. La integración no requiere ninguna configuración adicional en Security Hub, CSPM o Detective.

Para los hallazgos recibidos de otros Servicios de AWS, el panel de detalles de los hallazgos de la consola CSPM de Security Hub incluye una subsección Investiga en Detective. Esa subsección contiene un enlace a Detective, donde puede investigar más a fondo el problema de seguridad que indicó el resultado. También puede crear un gráfico de comportamiento en Detective basado en los hallazgos del CSPM de Security Hub para llevar a cabo investigaciones más eficaces. Para obtener más información, consulte [Resultados de seguridad de AWS](#) en la Guía de administración de Amazon Detective.

Si la agregación entre regiones está habilitada, al pasar de la región de agregación, Detective se abre en la región en la que se originó el resultado.

Si un enlace no funciona, para obtener información sobre la solución de problemas, consulte [Solución de problemas del pivot](#).

Amazon Security Lake (Recibe resultados)

Security Lake es un servicio de lago de datos de seguridad totalmente gestionado. Puede usar Amazon Security Lake para centralizar automáticamente los datos de seguridad de fuentes en la nube, en las instalaciones y personalizadas en un lago de datos almacenado en su cuenta. Los suscriptores pueden consumir datos de Security Lake para casos de uso de investigación y análisis.

Para activar esta integración, debe habilitar ambos servicios y agregar Security Hub CSPM como fuente en la consola de Security Lake, la API de Security Lake o. AWS CLI Una vez que complete estos pasos, Security Hub CSPM comenzará a enviar todos los hallazgos a Security Lake.

Security Lake normaliza automáticamente las conclusiones del CSPM de Security Hub y las convierte en un esquema estandarizado de código abierto denominado Open Cybersecurity Schema Framework (OCSF). En Security Lake, puede añadir uno o más suscriptores para consumir las conclusiones del CSPM de Security Hub.

Para obtener más información sobre esta integración, incluidas las instrucciones sobre cómo añadir Security Hub CSPM como fuente y crear suscriptores, consulte [Integración con AWS Security Hub Cloud Security Posture Management \(CSPM\) en la Guía del usuario](#) de Amazon Security Lake.

AWS Systems Manager Explorer y OpsCenter (recibe y actualiza los resultados)

AWS Systems Manager Explore y OpsCenter reciba las conclusiones del Security Hub CSPM y actualícelas en Security Hub CSPM.

Explorer le proporciona un panel personalizable con información y análisis clave sobre el estado y el rendimiento operativos de su entorno de AWS .

OpsCenter le proporciona una ubicación central para ver, investigar y resolver los elementos de trabajo operativos.

Para obtener más información sobre Explorer OpsCenter, consulte [Gestión de operaciones](#) en la Guía del AWS Systems Manager usuario.

AWS Trusted Advisor (Recibe los resultados)

Trusted Advisor se basa en las mejores prácticas aprendidas al atender a cientos de miles de AWS clientes. Trusted Advisor inspecciona su AWS entorno y, a continuación, hace recomendaciones cuando existen oportunidades para ahorrar dinero, mejorar la disponibilidad y el rendimiento del sistema o ayudar a cerrar las brechas de seguridad.

Al habilitar tanto Trusted Advisor el CSPM como el Security Hub, la integración se actualiza automáticamente.

Security Hub CSPM envía los resultados de sus comprobaciones de mejores prácticas de seguridad AWS fundamentales a. Trusted Advisor

Para obtener más información sobre la integración del Security Hub con el CSPM Trusted Advisor, consulte [Visualización de los controles de AWS Security Hub Cloud Security Posture Management \(CSPM\) en AWS Trusted Advisor](#) la Guía del usuario de Support AWS .

Integraciones de productos de terceros con Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (CSPM) se integra con varios productos de socios de terceros. Una integración puede realizar una o más de las siguientes acciones:

- Envíe las conclusiones que genere a Security Hub (CSPM)
- Reciba las conclusiones de Security Hub (CSPM)
- Actualización de los resultados en Security Hub (CSPM)

Las integraciones que envían los resultados a Security Hub CSPM tienen un Amazon Resource Name (ARN).

Es posible que una integración no esté disponible en todas. Regiones de AWS Si una integración no es compatible en la región en la que ha iniciado sesión actualmente en la consola CSPM de Security Hub, no aparecerá en la página de integraciones de la consola. Para obtener una lista de las integraciones que están disponibles en las regiones de China y AWS GovCloud (US) Regions, consulte [Disponibilidad de las integraciones por región](#).

<Si tiene una solución de seguridad y está interesado en convertirse en socio de Para obtener más información, consulte la Guía [AWS de integración para socios de Security Hub Cloud Security Posture Management \(CSPM\)](#).

Descripción general de las integraciones de terceros con Security Hub CSPM

Esta es una descripción general de las integraciones de terceros que envían las conclusiones al Security Hub CSPM o reciben las conclusiones del Security Hub CSPM:

Integración	Dirección	ARN (si corresponde)
3CORESec – 3CORESec NTA	Envía resultados	arn:aws:securityhub: <REGION>::product/3coresec/3coresec
Alert Logic – SIEMless Threat Management	Envía resultados	arn:aws:securityhub: <REGION>:733251395267:product/alertlogic/althreatmanagement
Aqua Security – Aqua Cloud Native Security Platform	Envía resultados	arn:aws:securityhub: <REGION>::product/aquasecurity/aquasecurity
Aqua Security – Kube-bench	Envía resultados	arn:aws:securityhub: <REGION>::product/aqua-security/kube-bench
Armor – Armor Anywhere	Envía resultados	arn:aws:securityhub: <REGION>:679703615338:product/armordefense/armoranywhere
AttackIQ – AttackIQ	Envía resultados	arn:aws:securityhub: <REGION>::product

Integración	Dirección	ARN (si corresponde)
		/attackiq/attackiq-platform
Barracuda Networks – Cloud Security Guardian	Envía resultados	arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian
BigID – BigID Enterprise	Envía resultados	arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise
Blue Hexagon – Blue Hexagon forAWS	Envía resultados	arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws
Check Point – CloudGuard IaaS	Envía resultados	arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas
Check Point – CloudGuard Posture Management	Envía resultados	arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc
Claroty – xDome	Envía resultados	arn:aws:securityhub:<REGION>::product/claroty/xdome

Integración	Dirección	ARN (si corresponde)
Cloud Storage Security – Antivirus for Amazon S3	Envía resultados	arn:aws:securityhub: <REGION>::product/cloud-storage-security/antivirus-for-amazon-s3
Contrast Security	Envía resultados	arn:aws:securityhub: <REGION>::product/contrast-security/security-assess
CrowdStrike – CrowdStrike Falcon	Envía resultados	arn:aws:securityhub: <REGION>:517716713836:product/crowdstrike/crowdstrike-falcon
CyberArk – Privileged Threat Analytics	Envía resultados	arn:aws:securityhub: <REGION>:749430749651:product/cyberark/cyberark-pta
Data Theorem – Data Theorem	Envía resultados	arn:aws:securityhub: <REGION>::product/data-theorem/api-cloud-web-secure
Drata	Envía resultados	arn:aws:securityhub: <REGION>::product/drata/drata-integration

Integración	Dirección	ARN (si corresponde)
Forcepoint – Forcepoint CASB	Envía resultados	arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-casb
Forcepoint – Forcepoint Cloud Security Gateway	Envía resultados	arn:aws:securityhub: <REGION>::product/forcepoint/forcepoint-cloud-security-gateway
Forcepoint – Forcepoint DLP	Envía resultados	arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-dlp
Forcepoint – Forcepoint NGFW	Envía resultados	arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-ngfw
Fugue – Fugue	Envía resultados	arn:aws:securityhub: <REGION>::product/fugue/fugue
Guardicore – Centra 4.0	Envía resultados	arn:aws:securityhub: <REGION>::product/guardicore/guardicore

Integración	Dirección	ARN (si corresponde)
HackerOne – Vulnerability Intelligence	Envía resultados	arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence
JFrog – Xray	Envía resultados	arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray
Juniper Networks – vSRX Next Generation Firewall	Envía resultados	arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall
k9 Security – Access Analyzer	Envía resultados	arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer
Lacework – Lacework	Envía resultados	arn:aws:securityhub:<REGION>::product/lacework/lacework
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	Envía resultados	arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws
NETSCOUT – NETSCOUT Cyber Investigator	Envía resultados	arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator

Integración	Dirección	ARN (si corresponde)
Palo Alto Networks – Prisma Cloud Compute	Envía resultados	arn:aws:securityhub: <REGION>:496947949261:product/twistlock/twistlock-enterprise
Palo Alto Networks – Prisma Cloud Enterprise	Envía resultados	arn:aws:securityhub: <REGION>:188619942792:product/paloaltonetworks/redlock
Plerion – Cloud Security Platform	Envía resultados	arn:aws:securityhub: <REGION>::product/plerion/cloud-security-platform
Prowler – Prowler	Envía resultados	arn:aws:securityhub: <REGION>::product/prowler/prowler
Qualys – Vulnerability Management	Envía resultados	arn:aws:securityhub: <REGION>:805950163170:product/qualys/qualys-vm
Rapid7 – InsightVM	Envía resultados	arn:aws:securityhub: <REGION>:336818582268:product/rapid7/insightvm
SecureCloudDB – SecureCloudDB	Envía resultados	arn:aws:securityhub: <REGION>::product/secureclouddb/secureclouddb

Integración	Dirección	ARN (si corresponde)
SentinelOne – SentinelOne	Envía resultados	arn:aws:securityhub: <REGION> ::product/sentinelone/endpoint-protection
Snyk	Envía resultados	arn:aws:securityhub: <region> ::product/snyk/snyk
Sonrai Security – Sonrai Dig	Envía resultados	arn:aws:securityhub: <REGION> ::product/sonrai-security/sonrai-dig
Sophos – Server Protection	Envía resultados	arn:aws:securityhub: <REGION> :062897671886:product/sophos/sophos-server-protection
StackRox – StackRox Kubernetes Security	Envía resultados	arn:aws:securityhub: <REGION> ::product/stackrox/kubernetes-security
Sumo Logic – Machine Data Analytics	Envía resultados	arn:aws:securityhub: <REGION> :956882708938:product/sumologicinc/sumologic-mda
Symantec – Cloud Workload Protection	Envía resultados	arn:aws:securityhub: <REGION> :754237914691:product/symantec-corp/symantec-cwp

Integración	Dirección	ARN (si corresponde)
Tenable – Tenable.io	Envía resultados	arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io
Trend Micro – Cloud One	Envía resultados	arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one
Vectra – Cognito Detect	Envía resultados	arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect
Wiz	Envía resultados	arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security
Atlassian - Jira Service Management	Recibe y actualiza resultados	No aplicable
Atlassian - Jira Service Management Cloud	Recibe y actualiza resultados	No aplicable
Atlassian – Opsgenie	Recibe resultados	No aplicable
Fortinet – FortiCNP	Recibe resultados	No aplicable
IBM – QRadar	Recibe resultados	No aplicable
Logz.io Cloud SIEM	Recibe resultados	No aplicable
MetricStream	Recibe resultados	No aplicable

Integración	Dirección	ARN (si corresponde)
MicroFocus – MicroFocus Arcsight	Recibe resultados	No aplicable
New Relic Vulnerability Management	Recibe resultados	No aplicable
PagerDuty – PagerDuty	Recibe resultados	No aplicable
Palo Alto Networks – Cortex XSOAR	Recibe resultados	No aplicable
Palo Alto Networks – VM-Series	Recibe resultados	No aplicable
Rackspace Technology – Cloud Native Security	Recibe resultados	No aplicable
Rapid7 – InsightConnect	Recibe resultados	No aplicable
RSA – RSA Archer	Recibe resultados	No aplicable
ServiceNow – ITSM	Recibe y actualiza resultados	No aplicable
Slack – Slack	Recibe resultados	No aplicable
Splunk – Splunk Enterprise	Recibe resultados	No aplicable
Splunk – Splunk Phantom	Recibe resultados	No aplicable
ThreatModeler	Recibe resultados	No aplicable
Trellix – Trellix Helix	Recibe resultados	No aplicable
Caveonix – Caveonix Cloud	Envía y recibe resultados	arn:aws:securityhub: <REGION> ::product/caveonix/caveonix-cloud

Integración	Dirección	ARN (si corresponde)
Cloud Custodian – Cloud Custodian	Envía y recibe resultados	arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian
DisruptOps, Inc. – DisruptOPS	Envía y recibe resultados	arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops
Kion	Envía y recibe resultados	arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio
Turbot – Turbot	Envía y recibe resultados	arn:aws:securityhub:<REGION>:453761072151:product/turbot/turbot

Integraciones de terceros que envían los resultados a Security Hub (CSPM)

Las siguientes integraciones de productos de socios externos envían los resultados a Security Hub CSPM. Security Hub CSPM transforma los hallazgos en el formato [AWS Security Finding](#).

3CORESec – 3CORESec NTA

Tipo de integración: Enviar

ARN del producto: arn:aws:securityhub:<REGION>::product/3coresec/3coresec

3CORESec proporciona servicios de detección gestionados tanto para sistemas en las instalaciones como de AWS. Su integración con Security Hub CSPM permite ver amenazas como el malware, la escalada de privilegios, el movimiento lateral y la segmentación inadecuada de la red.

[Enlace al producto](#)

[Documentación de socios](#)

Alert Logic – SIEMless Threat Management

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

Obtenga el nivel de cobertura adecuado: visibilidad de vulnerabilidades y activos, detección de amenazas y gestión de incidentes, y opciones asignadas de AWS WAF analistas de SOC.

[Enlace al producto](#)

[Documentación de socios](#)

Aqua Security – Aqua Cloud Native Security Platform

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP) proporciona seguridad durante todo el ciclo de vida de las aplicaciones basadas en contenedores y sin servidor, desde la CI/CD canalización hasta los entornos de producción en tiempo de ejecución.

[Enlace al producto](#)

[Documentación de socios](#)

Aqua Security – Kube-bench

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-bench es una herramienta de código abierto que ejecuta el Punto de referencia de Kubernetes del Center for Internet Security (Centro para la seguridad de Internet, CIS) con respecto a su entorno.

[Enlace al producto](#)

[Documentación de socios](#)

Armor – Armor Anywhere

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywhere ofrece seguridad gestionada y conformidad para AWS.

[Enlace al producto](#)

[Documentación de socios](#)

AttackIQ – AttackIQ

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platform emula un comportamiento adverso real conforme al marco MITRE ATT&CK para ayudarle a validar y mejorar su posición general de seguridad.

[Enlace al producto](#)

[Documentación de socios](#)

Barracuda Networks – Cloud Security Guardian

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentry ayuda a las organizaciones a mantener la seguridad al desarrollar aplicaciones y migrar cargas de trabajo hacia o desde la nube pública.

[AWS Enlace a Marketplace](#)

[Enlace al producto](#)

BigID – BigID Enterprise

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

La BigID Enterprise Privacy Management Platform ayuda a las empresas a gestionar y proteger sus datos confidenciales (PII) en todos sus sistemas.

[Enlace al producto](#)

[Documentación de socios](#)

Blue Hexagon— Blue Hexagon para AWS

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagon es una plataforma de detección de amenazas en tiempo real. Utiliza principios de aprendizaje profundo para detectar amenazas conocidas y desconocidas, como malware y anomalías en la red.

[AWS Enlace a Marketplace](#)

[Documentación de socios](#)

Check Point – CloudGuard IaaS

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuard amplía fácilmente la seguridad integral de prevención de amenazas y, al AWS mismo tiempo, protege los activos en la nube.

[Enlace al producto](#)

[Documentación de socios](#)

Check Point – CloudGuard Posture Management

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

Una plataforma SaaS que ofrece seguridad de la red en la nube verificable, protección de IAM avanzada y gobernanza y conformidad integrales.

[Enlace al producto](#)

[Documentación de socios](#)

Claroty – xDome

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDome ayuda a las organizaciones a proteger sus sistemas ciberfísicos en todo el Internet de las cosas (XIoT) extendido en entornos industriales (OT), sanitarios (IoMT) y empresariales (IoT).

[Enlace al producto](#)

[Documentación de socios](#)

Cloud Storage Security – Antivirus for Amazon S3

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Security proporciona análisis antivirus y antimalware nativos en la nube para objetos de Amazon S3.

Antivirus for Amazon S3 ofrece escaneos programados y en tiempo real de objetos y archivos en Amazon S3 para detectar malware y amenazas. Proporciona visibilidad y solución a los problemas y a los archivos infectados.

[Enlace al producto](#)

[Documentación de socios](#)

Contrast Security – Contrast Assess

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assesses una herramienta del IAST que permite detectar vulnerabilidades en tiempo real en aplicaciones web y microservicios. APIs Contrast Assesse integra con Security Hub CSPM para ayudar a proporcionar una visibilidad y una respuesta centralizadas para todas sus cargas de trabajo.

[Enlace al producto](#)

[Documentación de socios](#)

CrowdStrike – CrowdStrike Falcon

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

El sensor individual y ligero CrowdStrike Falcon unifica antivirus de próxima generación, detección y respuesta de punto de conexión y vigilancia administrada 24/7 a través de la nube.

[AWS Enlace a Marketplace](#)

[Documentación de socios](#)

CyberArk – Privileged Threat Analytics

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analytics recopila, detecta, alerta y responde a actividades y comportamiento de alto riesgo de las cuentas privilegiadas que podrían tener ataques en curso.

[Enlace al producto](#)

[Documentación de socios](#)

Data Theorem – Data Theorem

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theorem escanea continuamente las aplicaciones web y los recursos de la nube en busca de fallas de seguridad y brechas en la privacidad de los datos para evitar violaciones de AppSec datos. APIs

[Enlace al producto](#)

[Documentación de socios](#)

Drata

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drata es una plataforma de automatización del cumplimiento que le ayuda a lograr y mantener el cumplimiento de varios marcos SOC2, como la ISO y el GDPR. La integración entre el Security Hub CSPM Drata y el Security Hub le ayuda a centralizar sus hallazgos de seguridad en un solo lugar.

[AWS Enlace a Marketplace](#)

[Documentación de socios](#)

Forcepoint – Forcepoint CASB

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASB le permite detectar el uso de aplicaciones en la nube, analizar riesgos y aplicar controles adecuados para SaaS y aplicaciones personalizadas.

[Enlace al producto](#)[Documentación de socios](#)

Forcepoint – Forcepoint Cloud Security Gateway

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gateway es un servicio de seguridad en la nube convergente que proporciona visibilidad, control y protección contra amenazas a los usuarios y los datos, estén donde estén.

[Enlace al producto](#)[Documentación de socios](#)

Forcepoint – Forcepoint DLP

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLP aborda el riesgo centrado en el ser humano con visibilidad y control dondequiera que los empleados trabajen y donde residan los datos.

[Enlace al producto](#)[Documentación de socios](#)

Forcepoint – Forcepoint NGFW

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFW le permite conectar su AWS entorno a la red empresarial con la escalabilidad, la protección y los conocimientos necesarios para gestionar su red y responder a las amenazas.

[Enlace al producto](#)[Documentación de socios](#)

Fugue – Fugue

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugue es una plataforma nativa de la nube escalable y sin agentes que automatiza la validación continua infrastructure-as-code y el tiempo de ejecución de los entornos de ejecución en la nube mediante las mismas políticas.

[Enlace al producto](#)[Documentación de socios](#)

Guardicore – Centra 4.0

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centra proporciona visualización de flujo, microsegmentación y detección de interrupción para cargas de trabajo en los modernos centros de datos y nubes.

[Enlace al producto](#)[Documentación de socios](#)

HackerOne – Vulnerability Intelligence

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

La plataforma HackerOne se asocia con la comunidad mundial de hackers para descubrir los problemas de seguridad más relevantes. Vulnerability Intelligence permite a su organización ir más allá del escaneo automatizado. Comparte vulnerabilidades que los piratas informáticos éticos de HackerOne han validado y proporciona medidas para reproducirlas.

[AWS enlace al mercado](#)[Documentación de socios](#)

JFrog – Xray

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xray es una herramienta universal de análisis de la composición de software (Software Composition Analysis, SCA) para la seguridad de aplicaciones que escanea continuamente los archivos binarios para comprobar si cumplen con las licencias y si presentan vulnerabilidades de seguridad para que pueda ejecutar una cadena de suministro de software segura.

[AWS Enlace a Marketplace](#)[Documentación de socios](#)

Juniper Networks – vSRX Next Generation Firewall

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks' vSRX Virtual Next Generation Firewall ofrece un firewall virtual completo basado en la nube con seguridad avanzada, una SD-WAN segura, redes sólidas y automatización integrada.

[AWS Enlace a Marketplace](#)[Documentación de socios](#)[Enlace al producto](#)

k9 Security – Access Analyzer

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Securityte notifica cuando se producen cambios de acceso importantes en tu AWS Identity and Access Management cuenta. Con élk9 Security, puede comprender el acceso que tienen los usuarios y las funciones de IAM a sus datos críticos Servicios de AWS y a sus datos.

k9 Securityestá diseñado para ofrecer servicios continuos, lo que le permite poner en práctica la IAM con auditorías de acceso prácticas y una automatización sencilla de las políticas para Terraform. AWS CDK

[Enlace al producto](#)

[Documentación de socios](#)

Lacework – Lacework

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Lacework es la plataforma de seguridad basada en datos para la nube. La plataforma de seguridad en la nube Lacework automatiza la seguridad en la nube a escala para que pueda innovar con rapidez y seguridad.

[Enlace al producto](#)

[Documentación de socios](#)

McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP) ofrece la gestión de la postura de seguridad en la nube (Cloud Security Posture Management, CSPM) y la plataforma de protección de la carga de trabajo en la nube (Cloud Workload Protection Platform, CWPP) para su entorno de AWS .

[Enlace al producto](#)

[Documentación de socios](#)

NETSCOUT – NETSCOUT Cyber Investigator

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigator es una plataforma empresarial de análisis forense, investigación de riesgos y amenazas a la red que ayuda a reducir el impacto de las ciberamenazas en las empresas.

[Enlace al producto](#)

[Documentación de socios](#)

Palo Alto Networks – Prisma Cloud Compute

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Compute es una plataforma de ciberseguridad nativa de la nube que protege los contenedores VMs y las plataformas sin servidor.

[Enlace al producto](#)

[Documentación de socios](#)

Palo Alto Networks – Prisma Cloud Enterprise

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

Protege su AWS despliegue con análisis de seguridad en la nube, detección avanzada de amenazas y supervisión del cumplimiento.

[Enlace al producto](#)

[Documentación de socios](#)

Plerion – Cloud Security Platform

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerion es una plataforma de seguridad en la nube con un enfoque único orientado a las amenazas y al riesgo que ofrece medidas preventivas, de inspección y correctivas en todas sus cargas de trabajo. La integración entre Security Hub CSPM Plerion y Security Hub permite a los clientes centralizar sus hallazgos de seguridad y actuar en función de ellos en un solo lugar.

[AWS Enlace a Marketplace](#)

[Documentación de socios](#)

Prowler – Prowler

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowler es una herramienta de seguridad de código abierto para realizar AWS comprobaciones relacionadas con las mejores prácticas de seguridad, el refuerzo y la supervisión continua.

[Enlace al producto](#)

[Documentación de socios](#)

Qualys – Vulnerability Management

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM) escanea e identifica continuamente las vulnerabilidades, protegiendo sus activos.

[Enlace al producto](#)

[Documentación de socios](#)

Rapid7 – InsightVM

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVM proporciona administración de vulnerabilidades para entornos modernos, lo que le permite encontrar, priorizar y remediar las vulnerabilidades de manera eficiente.

[Enlace al producto](#)

[Documentación de socios](#)

SecureCloudDB – SecureCloudDB

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/secureclouddb/secureclouddb`

SecureCloudDB es una herramienta de seguridad de bases de datos nativa en la nube que proporciona una visibilidad completa de las posiciones y actividades de seguridad internas y externas. Detecta infracciones de seguridad y corrige vulnerabilidades en las bases de datos explotables.

[Enlace al producto](#)

[Documentación de socios](#)

SentinelOne – SentinelOne

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOne es una plataforma autónoma de detección y respuesta ampliadas (XDR) que abarca la prevención, la detección, la respuesta y la búsqueda impulsadas por IA en puntos de conexión, contenedores, cargas de trabajo en la nube y dispositivos de IoT.

[AWS Enlace a Marketplace](#)

[Enlace al producto](#)

Snyk

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snyk proporciona una plataforma de seguridad que analiza componentes de aplicaciones para detectar riesgos de seguridad en las cargas de trabajo que se estén ejecutando en AWS. Estos riesgos se envían al Security Hub CSPM en forma de hallazgos, lo que ayuda a los desarrolladores y equipos de seguridad a visualizarlos y priorizarlos junto con el resto de sus hallazgos de AWS seguridad.

[AWS Enlace a Marketplace](#)[Documentación de socios](#)

Sonrai Security – Sonrai Dig

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Dig supervisa y corrige las configuraciones incorrectas de la nube y las infracciones de las políticas para que pueda mejorar su posición de seguridad y conformidad.

[Enlace al producto](#)[Documentación de socios](#)

Sophos – Server Protection

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protection defiende las aplicaciones y los datos críticos que constituyen el núcleo de su organización mediante defense-in-depth técnicas integrales.

[Enlace al producto](#)

StackRox – StackRox Kubernetes Security

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRox ayuda a las empresas a proteger sus implementaciones de contenedores y Kubernetes a escala al aplicar sus políticas de conformidad y seguridad a lo largo de todo el ciclo de vida de los contenedores: creación, implementación y ejecución.

[Enlace al producto](#)[Documentación de socios](#)

Sumo Logic – Machine Data Analytics

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logic es una segura plataforma de análisis de datos de las máquinas que permite a los equipos de operaciones de crear, ejecutar y proteger sus aplicaciones de AWS .

[Enlace al producto](#)[Documentación de socios](#)

Symantec – Cloud Workload Protection

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protection proporciona una protección completa para sus EC2 instancias de Amazon con antimalware, prevención de intrusiones y supervisión de la integridad de los archivos.

[Enlace al producto](#)

[Documentación de socios](#)

Tenable – Tenable.io

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

Puede identificar, investigar y priorizar las vulnerabilidades con precisión. Administrado en la nube.

[Enlace al producto](#)

[Documentación de socios](#)

Trend Micro – Cloud One

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud One proporciona la información de seguridad correcta a los equipos en el momento y lugar correctos. Esta integración envía los resultados de seguridad al Security Hub CSPM en tiempo real, lo que mejora la visibilidad de AWS los recursos y los detalles de los Trend Micro Cloud One eventos en Security Hub CSPM.

[AWS Enlace a Marketplace](#)

[Documentación de socios](#)

Vectra – Cognito Detect

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectra está transformando la ciberseguridad mediante la aplicación de IA avanzada para detectar y responder a los ciberatacantes ocultos antes de que puedan robar o causar daños.

[AWS Enlace a Marketplace](#)

[Documentación de socios](#)

Wiz – Wiz Security

Tipo de integración: Enviar

ARN del producto: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wiz analiza continuamente las configuraciones, las vulnerabilidades, las redes, la configuración de IAM, los secretos y mucho más en sus Cuentas de AWS usuarios y cargas de trabajo para descubrir problemas críticos que representan un riesgo real. Integre Wiz con Security Hub CSPM para visualizar y responder a los problemas que Wiz detecta desde la consola CSPM de Security Hub.

[AWS Enlace a Marketplace](#)

[Documentación de socios](#)

Integraciones de terceros que reciben las conclusiones de Security Hub (CSPM)

Las siguientes integraciones de productos de socios externos reciben las conclusiones de Security Hub CSPM. Si se indica lo contrario, es posible que el producto también actualice los resultados. En este caso, las actualizaciones que realice en los hallazgos del producto asociado también se reflejan en Security Hub CSPM.

Atlassian - Jira Service Management

Tipo de integración: Recibir y actualizar

El formulario Jira envía AWS Service Management Connector los resultados desde el Security Hub CSPM a. Jira Jira los problemas se crean en función de los hallazgos. Cuando se actualizan los Jira problemas, las conclusiones correspondientes se actualizan en Security Hub CSPM.

La integración solo es compatible con Jira Server y Jira Data Center.

Para obtener una descripción general de la integración y su funcionamiento, vea el vídeo [AWS Security Hub Cloud Security Posture Management \(CSPM\): integración bidireccional](#) con. Atlassian Jira Service Management

[Enlace al producto](#)

[Documentación de socios](#)

Atlassian - Jira Service Management Cloud

Tipo de integración: Recibir y actualizar

Jira Service Management Cloud es el componente de nube de Jira Service Management.

El formulario Jira envía AWS Service Management Connector los resultados desde el Security Hub CSPM a Jira. Los resultados desencadenan la creación de problemas en Jira Service Management Cloud. Al actualizar esos problemas en Jira Service Management Cloud, las conclusiones correspondientes también se actualizan en Security Hub CSPM.

[Enlace al producto](#)

[Documentación de socios](#)

Atlassian – Opsgenie

Tipo de integración: Recibir

Opsgenie es una moderna solución de administración de incidentes para servicios siempre en funcionamiento, que permite a los equipos de desarrollo y operaciones planear interrupciones del servicio y mantener el control durante incidentes.

La integración con Security Hub CSPM garantiza que los incidentes críticos relacionados con la seguridad se envíen a los equipos correspondientes para su resolución inmediata.

[Enlace al producto](#)

[Documentación de socios](#)

Fortinet – FortiCNP

Tipo de integración: Recibir

FortiCNP es un producto de protección nativo en la nube que agrupa los resultados de seguridad en información procesable y prioriza la información de seguridad en función de la puntuación de riesgo para reducir la fatiga de alertas y acelerar la corrección.

[AWS Enlace a Marketplace](#)

[Documentación de socios](#)

IBM – QRadar

Tipo de integración: Recibir

IBM QRadar de SIEM proporciona a los equipos de seguridad una forma rápida y precisa de detectar, priorizar, investigar y responder a las amenazas.

[Enlace al producto](#)

[Documentación de socios](#)

Logz.io Cloud SIEM

Tipo de integración: Recibir

Logz.io es un proveedor de Cloud SIEM que proporciona una correlación avanzada de los datos de registro y eventos para ayudar a los equipos de seguridad a detectar, analizar y responder a las amenazas de seguridad en tiempo real.

[Enlace al producto](#)

[Documentación de socios](#)

MetricStream – CyberGRC

Tipo de integración: Recibir

MetricStream CyberGRC le ayuda a gestionar, medir y mitigar los riesgos de ciberseguridad. Al recibir las conclusiones del CSPM de Security Hub, CyberGRC proporciona una mayor visibilidad de estos riesgos, de modo que puede priorizar las inversiones en ciberseguridad y cumplir con las políticas de TI.

[AWS Enlace a Marketplace](#)

[Enlace al producto](#)

MicroFocus – MicroFocus Arcsight

Tipo de integración: Recibir

ArcSight acelera la detección y la respuesta efectivas a las amenazas en tiempo real, integrando la correlación de eventos y los análisis supervisados y no supervisados con la automatización y la orquestación de las respuestas.

[Enlace al producto](#)

[Documentación de socios](#)

New Relic Vulnerability Management

Tipo de integración: Recibir

New Relic Vulnerability Management recibe las conclusiones de seguridad de Security Hub CSPM, por lo que puede obtener una visión centralizada de la seguridad junto con la telemetría del rendimiento en contexto en todo su conjunto.

[AWS Enlace a Marketplace](#)

[Documentación de socios](#)

PagerDuty – PagerDuty

Tipo de integración: Recibir

La plataforma de administración de operaciones digitales PagerDuty permite a los equipos mitigar proactivamente los problemas que afectan a los clientes, dirigiendo automáticamente cualquier señal a las acciones e información adecuadas.

AWS los usuarios pueden usar el PagerDuty conjunto de AWS integraciones para escalar sus entornos AWS y los híbridos con confianza.

Cuando se combina con las alertas de seguridad agrupadas y organizadas (CSPM) de Security PagerDuty Hub, los equipos pueden automatizar su proceso de respuesta a las amenazas y configurar rápidamente acciones personalizadas para evitar posibles problemas.

Los usuarios de PagerDuty que llevan a cabo un proyecto de migración a la nube pueden moverlo rápidamente, a la vez que se disminuye el impacto de los problemas que se producen durante todo el ciclo de vida de la migración.

[Enlace al producto](#)

[Documentación de socios](#)

Palo Alto Networks – Cortex XSOAR

Tipo de integración: Recibir

Cortex XSOAR es una plataforma de orquestación, automatización y respuesta de seguridad (SOAR) que se integra con toda la pila de productos de seguridad para acelerar la respuesta ante incidentes y las operaciones de seguridad.

[Enlace al producto](#)

[Documentación de socios](#)

Palo Alto Networks – VM-Series

Tipo de integración: Recibir

Palo Alto VM-Series al integrarse con Security Hub, el CSPM recopila información sobre amenazas y la envía al firewall de VM-Series próxima generación como una actualización automática de la política de seguridad que bloquea la actividad de direcciones IP maliciosas.

[Enlace al producto](#)

[Documentación de socios](#)

Rackspace Technology – Cloud Native Security

Tipo de integración: Recibir

Rackspace Technology ofrece servicios de seguridad administrados además de productos de seguridad nativos de AWS para el monitoreo las 24 horas del día, los 7 días de la semana, los 365 días del año por parte de Rackspace SOC, análisis avanzado y mitigación de amenazas.

[Enlace al producto](#)

Rapid7 – InsightConnect

Tipo de integración: Recibir

Rapid7 InsightConnect es una solución de automatización y orquestación de seguridad que permite a su equipo optimizar las operaciones SOC con poco o ningún código.

[Enlace al producto](#)

[Documentación de socios](#)

RSA – RSA Archer

Tipo de integración: Recibir

RSA Archer IT and Security Risk Management le permite determinar qué activos son fundamentales para su empresa, establecer y comunicar políticas y estándares de seguridad, detectar y responder a ataques, identificar y corregir deficiencias de seguridad y establecer prácticas recomendadas claras sobre gestión de riesgos de TI.

[Enlace al producto](#)

[Documentación de socios](#)

ServiceNow – ITSM

Tipo de integración: Recibir y actualizar

La ServiceNow integración con el Security Hub CSPM permite ver en él los hallazgos de seguridad del Security Hub CSPM. ServiceNow ITSM También puede configurarlo ServiceNow para que cree automáticamente un incidente o un problema cuando reciba un hallazgo del Security Hub CSPM.

Cualquier actualización de estos incidentes y problemas se traducirá en actualizaciones de los hallazgos de Security Hub CSPM.

Para obtener una descripción general de la integración y su funcionamiento, vea el vídeo [AWS Security Hub Cloud Security Posture Management \(CSPM\): integración bidireccional](#) con.

ServiceNow ITSM

[Enlace al producto](#)

[Documentación de socios](#)

Slack – Slack

Tipo de integración: Recibir

Slack es una capa de la pila de tecnología empresarial que reúne personas, datos y aplicaciones. Conformar un lugar integral donde las personas pueden trabajar juntas de forma eficaz, encontrar información importante y acceder a cientos de miles de aplicaciones y servicios críticos para dar lo mejor en su trabajo.

[Enlace al producto](#)

[Documentación de socios](#)

Splunk – Splunk Enterprise

Tipo de integración: Recibir

Splunk utiliza Amazon CloudWatch Events como consumidor de las conclusiones del CSPM de Security Hub. Envíe sus datos a Splunk para un análisis de seguridad avanzado y SIEM.

[Enlace al producto](#)

[Documentación de socios](#)

Splunk – Splunk Phantom

Tipo de integración: Recibir

Con la Splunk Phantom aplicación AWS Security Hub Cloud Security Posture Management (CSPM), los resultados se envían a Phantom para enriquecer el contexto de forma automatizada con información adicional de inteligencia sobre amenazas o para realizar acciones de respuesta automatizadas.

[Enlace al producto](#)

[Documentación de socios](#)

ThreatModeler

Tipo de integración: Recibir

ThreatModeler es una solución de modelado de amenazas automatizada que protege y amplía el ciclo de vida del desarrollo del software empresarial y la nube.

[Enlace al producto](#)

[Documentación de socios](#)

Trellix – Trellix Helix

Tipo de integración: Recibir

Trellix Helix es una plataforma de operaciones de seguridad alojada en la nube que permite a las organizaciones tomar el control de cualquier incidente, desde la alerta hasta la solución.

[Enlace al producto](#)

[Documentación de socios](#)

Integraciones de terceros que envían y reciben las conclusiones de Security Hub (CSPM)

Las siguientes integraciones de productos de socios externos envían y reciben las conclusiones de Security Hub CSPM.

Caveonix – Caveonix Cloud

Tipo de integración: Enviar y recibir

ARN del producto: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

La plataforma Caveonix basada en la inteligencia artificial automatiza la visibilidad, la evaluación y la mitigación en las nubes híbridas y abarca los servicios y contenedores nativos de la nube. VMs Integrado con AWS Security Hub Cloud Security Posture Management (CSPM), Caveonix combina AWS datos y análisis avanzados para obtener información sobre las alertas de seguridad y el cumplimiento.

[AWS Enlace a Marketplace](#)

[Documentación de socios](#)

Cloud Custodian – Cloud Custodian

Tipo de integración: Enviar y recibir

ARN del producto: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodian permite a los usuarios estar bien administrados en la nube. El sencillo DSL de YAML permite que unas reglas fácilmente definidas habiliten una infraestructura de nube bien administrada, segura y optimizada en costos.

[Enlace al producto](#)

[Documentación de socios](#)

DisruptOps, Inc. – DisruptOPS

Tipo de integración: Enviar y recibir

ARN del producto: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

La plataforma de operaciones de seguridad DisruptOps ayuda a las organizaciones a mantener las prácticas recomendadas de seguridad en la nube utilizando barreras de protección automatizadas.

[Enlace al producto](#)

[Documentación de socios](#)

Kion

Tipo de integración: Enviar y recibir

ARN del producto: `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion(anteriormente cloudtamer.io) es una solución completa de gobierno de la nube para. AWSKionofrece a las partes interesadas visibilidad de las operaciones en la nube y ayuda a los usuarios de la nube a gestionar las cuentas, controlar el presupuesto y los costes y garantizar el cumplimiento continuo.

[Enlace al producto](#)

[Documentación de socios](#)

Turbot – Turbot

Tipo de integración: Enviar y recibir

ARN del producto: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbot garantiza que la infraestructura de la nube sea segura, conforme, escalable y rentable.

[Enlace al producto](#)

[Documentación de socios](#)

Integración de Security Hub CSPM con productos personalizados

Además de las conclusiones generadas por AWS los servicios integrados y los productos de terceros, AWS Security Hub Cloud Security Posture Management (CSPM) puede consumir las conclusiones generadas por otros productos de seguridad personalizados.

Puede enviar estos resultados a Security Hub CSPM mediante el [BatchImportFindings](#) funcionamiento de la API CSPM de Security Hub. Puede utilizar la misma operación para actualizar las conclusiones de los productos personalizados que ya ha enviado a Security Hub CSPM.

Al configurar la integración personalizada, utilice [las directrices y listas de verificación](#) que se proporcionan en la Guía de integración de socios de CSPM de Security Hub.

Requisitos y recomendaciones para las integraciones de productos personalizados

Antes de poder invocar correctamente la operación de [BatchImportFindings](#) API, debe habilitar el CSPM de Security Hub.

También debe proporcionar detalles sobre los resultados del producto personalizado con el [the section called “Formato de búsqueda: ASFF”](#). Revise los siguientes requisitos y recomendaciones para las integraciones de productos personalizados:

Configuración del ARN del producto

Al habilitar el CSPM de Security Hub, se genera un producto predeterminado llamado Amazon Resource Name (ARN) para el CSPM de Security Hub en su cuenta corriente.

Este ARN del producto tiene el siguiente formato:

arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default. Por ejemplo, arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default.

Utilice este ARN del producto como el valor para el atributo [ProductArn](#) al invocar la operación de la API BatchImportFindings.

Configuración de los nombres de la empresa y los productos

Se puede utilizar `BatchImportFindings` para establecer un nombre de empresa y un nombre de producto preferidos para la integración personalizada que envía los resultados a Security Hub CSPM.

Los nombres especificados sustituyen al nombre de la empresa y al nombre del producto preconfigurados, denominados nombre personal y nombre predeterminado, respectivamente, y aparecen en la consola CSPM de Security Hub y en el JSON de cada hallazgo. Consulte [BatchImportFindings para encontrar proveedores](#).

Definir el hallazgo IDs

Debe proporcionar, gestionar e incrementar su propio hallazgo mediante IDs el [Id](#) atributo.

Cada nuevo resultado debería tener un ID de resultado único. Si el producto personalizado envía varios resultados con el mismo ID de búsqueda, Security Hub CSPM solo procesa el primer hallazgo.

Establecer el ID de cuenta

Debe especificar su propio ID de cuenta, utilizando el atributo [AwsAccountId](#).

Establecer las fechas creadas en y actualizadas en las fechas

Debe proporcionar sus propias marcas de tiempo para los atributos [CreatedAt](#) y [UpdatedAt](#).

Actualización de los resultados de los productos personalizados

Además de enviar los nuevos resultados de los productos personalizados, también puede utilizar la operación de la API [BatchImportFindings](#) para actualizar los resultados existentes de los productos personalizados.

Para actualizar los resultados existentes, utilice el ID del resultado existente (a través del atributo [Id](#)). Vuelva a enviar el resultado completo con la información adecuada actualizada en la solicitud, incluida una marca de tiempo [UpdatedAt](#) modificada.

Integraciones personalizadas de ejemplo

Puede utilizar los siguientes ejemplos de integraciones de productos personalizados como guía para crear su propia solución personalizada:

Envío de los resultados de los Chef InSpec escaneos a Security Hub (CSPM)

Puede crear una AWS CloudFormation plantilla que ejecute un análisis de [Chef InSpec](#) conformidad y, a continuación, envíe los resultados a Security Hub CSPM.

Para obtener más información, consulte [Supervisión continua del cumplimiento con Chef InSpecAWS Security Hub Cloud Posture Management \(CSPM\)](#).

Envío de las vulnerabilidades de los contenedores detectadas por el Trivy Security Hub (CSPM)

Puede crear una AWS CloudFormation plantilla que se utilice [AquaSecurity Trivy](#) para analizar los contenedores en busca de vulnerabilidades y, a continuación, enviar esas conclusiones de vulnerabilidad a Security Hub CSPM.

Para obtener más información, consulte [Cómo crear una CI/CD canalización para el escaneo de vulnerabilidades de contenedores con TrivyAWS Security Hub Cloud Security Posture Management \(CSPM\)](#).

Creación y actualización de los hallazgos en Security Hub (CSPM)

En AWS Security Hub Cloud Security Posture Management (CSPM), un hallazgo es un registro observable de un control de seguridad o una detección relacionada con la seguridad. Un hallazgo puede provenir de una de las siguientes fuentes:

- Una comprobación de seguridad para un control en Security Hub CSPM.
- Una integración con otro. Servicio de AWS
- Una integración con un producto de terceros.
- Una integración personalizada.

Security Hub CSPM normaliza los hallazgos de todas las fuentes en una sintaxis y un formato estándar denominados AWS Security Finding Format (ASFF). Para obtener información detallada sobre este formato, incluidas las descripciones de los campos ASFF individuales, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#). Si habilita la agregación entre regiones, Security Hub CSPM también agrega automáticamente los hallazgos nuevos y actualizados de todas las regiones vinculadas a la región de agregación que especifique. Para obtener más información, consulte [Descripción de la agregación entre regiones en Security Hub CSPM](#).

Una vez creada una búsqueda, se puede actualizar de la siguiente manera:

- Un proveedor de búsquedas puede usar el [BatchImportFindings](#) funcionamiento de la API CSPM de Security Hub para actualizar la información general sobre la búsqueda. Los proveedores de hallazgos solo pueden actualizar los hallazgos que hayan creado.
- Un cliente puede usar la consola CSPM de Security Hub o el [BatchUpdateFindings](#) funcionamiento de la API CSPM de Security Hub para actualizar el estado de la investigación sobre el hallazgo. La BatchUpdateFindings operación también puede ser utilizada por un SIEM, la emisión de tickets, la gestión de incidentes, la SOAR u otro tipo de herramienta en nombre de un cliente.

Para reducir el ruido de las búsquedas y agilizar el seguimiento y el análisis de los hallazgos individuales, Security Hub CSPM elimina automáticamente los hallazgos que no se hayan actualizado recientemente. El momento en que Security Hub CSPM lo hace depende de si el hallazgo está activo o archivado:

- Un hallazgo activo es aquel cuyo estado de registro () RecordState es. ACTIVE Security Hub CSPM almacena los hallazgos activos durante 90 días. Si un hallazgo activo no se ha actualizado durante 90 días, caduca y Security Hub CSPM lo elimina permanentemente.
- Un hallazgo archivado es un hallazgo cuyo estado de registro () es. RecordState ARCHIVED Security Hub CSPM almacena los hallazgos archivados durante 30 días. Si un hallazgo archivado no se ha actualizado durante 30 días, caduca y Security Hub CSPM lo elimina permanentemente.

En el caso de los hallazgos de control, que son los hallazgos que Security Hub CSPM genera a partir de las comprobaciones de seguridad de los controles, Security Hub CSPM determina si un hallazgo ha caducado en función del valor del UpdatedAt campo del hallazgo. Si este valor es de hace más de 90 días para un hallazgo activo, Security Hub CSPM elimina el hallazgo de forma permanente. Si este valor fue hace más de 30 días para un hallazgo archivado, Security Hub CSPM lo elimina permanentemente.

Para todos los demás tipos de hallazgos, Security Hub CSPM determina si un hallazgo ha caducado en función de los valores de los UpdatedAt campos ProcessedAt y del hallazgo. Security Hub CSPM compara los valores de estos campos y determina cuál es más reciente. Si el valor más reciente de un hallazgo activo es de hace más de 90 días, Security Hub CSPM elimina el hallazgo de forma permanente. Si el valor más reciente fue de hace más de 30 días para un hallazgo archivado, Security Hub CSPM elimina el hallazgo de forma permanente. La búsqueda de proveedores puede cambiar el valor del UpdatedAt campo de uno o más hallazgos mediante el [BatchImportFindings](#) funcionamiento de la API CSPM de Security Hub.

Para conservar los hallazgos a más largo plazo, puede exportarlos a un bucket de S3. Puedes hacerlo mediante una acción personalizada con una EventBridge regla de Amazon. Para obtener más información, consulte [Uso EventBridge para respuesta y remediación automatizadas](#).

Temas

- [BatchImportFindings para encontrar proveedores](#)
- [BatchUpdateFindings para clientes](#)
- [Revisión de los detalles y el historial de búsquedas en Security Hub \(CSPM\)](#)
- [Filtrado de resultados en Security Hub \(CSPM\)](#)
- [Agrupación de hallazgos en Security Hub \(CSPM\)](#)
- [Configuración del estado del flujo de trabajo de los hallazgos en Security Hub \(CSPM\)](#)
- [Enviar los resultados a un Security Hub \(CSPM\) personalizado \(acción\)](#)
- [AWS Formato de búsqueda de seguridad \(ASFF\)](#)

BatchImportFindings para encontrar proveedores

La búsqueda de proveedores puede utilizar la [BatchImportFindings](#) operación para crear nuevos hallazgos en AWS Security Hub Cloud Security Posture Management (CSPM). También pueden usar esta operación para actualizar las conclusiones que hayan creado. Al buscar proveedores, no se pueden actualizar los hallazgos que ellos no crearon.

Los clientes SIEMs, la venta de entradas, la SOAR y otros tipos de herramientas deben utilizar esta [BatchUpdateFindings](#) operación para realizar actualizaciones relacionadas con su investigación de los resultados obtenidos al encontrar proveedores. Para obtener más información, consulte [the section called “BatchUpdateFindings para clientes”](#).

Cuando Security Hub CSPM recibe una BatchImportFindings solicitud para crear o actualizar un hallazgo, genera automáticamente un Security Hub Findings - Imported evento en Amazon. EventBridge Puede tomar medidas automatizadas en relación con ese evento. Para obtener más información, consulte [the section called “Respuesta y corrección automatizadas”](#).

Requisitos previos para utilizar BatchImportFindings

BatchImportFindings debe ser llamada por una de las siguientes opciones:

- La cuenta que está asociada al resultado. El identificador de la cuenta asociada debe coincidir con el valor del atributo `AwsAccountId` del resultado.
- Una cuenta que figura en la lista de permitidos como integración oficial de socios de CSPM de Security Hub.

Security Hub CSPM solo puede aceptar la búsqueda de actualizaciones para cuentas que tengan activado Security Hub CSPM. El proveedor de hallazgos también debe estar habilitado. Si el CSPM de Security Hub está deshabilitado o la integración del proveedor de búsqueda no está habilitada, los hallazgos se muestran en la `FailedFindings` lista con un `InvalidAccess` error.

Determinación de si se debe crear o actualizar un hallazgo

Para determinar si se debe crear o actualizar un hallazgo, Security Hub CSPM comprueba el `ID` campo. Si el valor de `ID` no coincide con un hallazgo existente, Security Hub CSPM crea un nuevo hallazgo.

Si `ID` coincide con un hallazgo existente, Security Hub CSPM comprueba el `UpdatedAt` campo para ver si hay una actualización y procede de la siguiente manera:

- Si `UpdatedAt` la actualización coincide con el hallazgo existente o se produce antes `UpdatedAt`, Security Hub CSPM ignora la solicitud de actualización.
- Si `UpdatedAt` la actualización se produce después `UpdatedAt` del hallazgo existente, Security Hub CSPM actualiza el hallazgo existente.

Restricciones para la actualización de resultados con **BatchImportFindings**

Los proveedores de resultados no pueden utilizar `BatchImportFindings` para actualizar los siguientes atributos de un resultado existente:

- `Note`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Security Hub CSPM ignora cualquier contenido proporcionado en una `BatchImportFindings` solicitud de estos atributos. Los clientes o las entidades que actúan en su nombre (como las herramientas de creación de tickets) pueden utilizar `BatchUpdateFindings` para actualizar estos atributos.

Actualizar los resultados mediante `FindingProviderFields`

La búsqueda de proveedores tampoco debería servir `BatchImportFindings` para actualizar los siguientes atributos de nivel superior en el formato de búsqueda de AWS seguridad (ASFF):

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

En su lugar, los proveedores de resultados deben utilizar el objeto [FindingProviderFields](#) para proporcionar valores para estos atributos.

Ejemplo

```
"FindingProviderFields": {
  "Confidence": 42,
  "Criticality": 99,
  "RelatedFindings": [
    {
      "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000"
    }
  ],
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

En el caso de `BatchImportFindings` las solicitudes, Security Hub CSPM gestiona los valores de los atributos de nivel superior y de la siguiente manera [FindingProviderFields](#).

(Preferido) **BatchImportFindings** proporciona un valor para un atributo [FindingProviderFields](#), pero no proporciona un valor para el atributo de nivel superior correspondiente.

Por ejemplo, `BatchImportFindings` proporciona `FindingProviderFields.Confidence`, pero no proporciona `Confidence`. Esta es la opción preferida para las solicitudes `BatchImportFindings`.

Security Hub CSPM actualiza el valor del atributo en `FindingProviderFields`

Replica el valor en el atributo de nivel superior solo si `BatchUpdateFindings` aún no actualizó el atributo.

BatchImportFindings proporciona un valor para un atributo de nivel superior, pero no proporciona un valor para el atributo correspondiente **FindingProviderFields**.

Por ejemplo, `BatchImportFindings` proporciona `Confidence`, pero no proporciona `FindingProviderFields.Confidence`.

Security Hub CSPM utiliza el valor para actualizar el atributo en `FindingProviderFields`. Sobrescribe cualquier valor existente.

El CSPM de Security Hub actualiza el atributo de nivel superior solo si el atributo aún no lo ha actualizado. `BatchUpdateFindings`

BatchImportFindings proporciona un valor tanto para un atributo de nivel superior como para el atributo correspondiente a **FindingProviderFields**.

Por ejemplo, `BatchImportFindings` proporciona tanto `Confidence` como `FindingProviderFields.Confidence`.

Si se trata de un nuevo hallazgo, el CSPM de Security Hub utiliza el valor in `FindingProviderFields` para rellenar tanto el atributo de nivel superior como el atributo correspondiente. `FindingProviderFields` No utiliza el valor de atributo de nivel superior proporcionado.

Para un hallazgo existente, el CSPM de Security Hub utiliza ambos valores. Sin embargo, actualiza el valor del atributo de nivel superior solo si `BatchUpdateFindings` aún no ha actualizado el atributo.

BatchUpdateFindings para clientes

AWS Los clientes de Security Hub Cloud Security Posture Management (CSPM) y las entidades que actúen en su nombre pueden utilizar la [BatchUpdateFindings](#) operación para actualizar la información relacionada con el procesamiento de las conclusiones del Security Hub CSPM a partir de la búsqueda de proveedores. Como cliente, puede utilizar esta operación directamente. Las herramientas SIEM, de emisión de billetes, de gestión de incidentes y de SOAR también pueden utilizar esta operación en nombre de un cliente.

No puede utilizar la `BatchUpdateFindings` operación para crear nuevos hallazgos. Sin embargo, puede utilizarla para actualizar hasta 100 hallazgos existentes a la vez. En una `BatchUpdateFindings` solicitud, se especifican los resultados que se van a actualizar, los campos del formato de búsqueda de AWS seguridad (ASFF) que se van a actualizar para los resultados y los nuevos valores de los campos. A continuación, Security Hub CSPM actualiza los resultados tal y como se especifica en su solicitud. Este proceso puede tardar varios minutos. Si actualiza las conclusiones mediante la `BatchUpdateFindings` operación, las actualizaciones no afectarán a los valores existentes en el `UpdatedAt` campo de las conclusiones.

Cuando Security Hub CSPM recibe una `BatchUpdateFindings` solicitud para actualizar un hallazgo, genera automáticamente un Security Hub Findings – Imported evento en Amazon. EventBridge Si lo desea, puede utilizar este evento para tomar medidas automatizadas en relación

con el hallazgo especificado. Para obtener más información, consulte [the section called “Respuesta y corrección automatizadas”](#).

Campos disponibles para BatchUpdateFindings

Si ha iniciado sesión en una cuenta de administrador CSPM de Security Hub, puede utilizarla BatchUpdateFindings para actualizar las conclusiones generadas por la cuenta de administrador o las cuentas de los miembros. Las cuentas de miembro pueden utilizar BatchUpdateFindings para actualizar los resultados solo para su cuenta.

Los clientes pueden usar BatchUpdateFindings para actualizar los siguientes campos y objetos:

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

Configuración del acceso a BatchUpdateFindings

Puede configurar políticas AWS Identity and Access Management (IAM) para restringir el acceso y actualizar los campos de búsqueda y los valores de los campos. BatchUpdateFindings

En una declaración para restringir el acceso a BatchUpdateFindings, utilice los siguientes valores:

- Action es securityhub:BatchUpdateFindings
- Effect es Deny
- Para Condition, puede denegar una solicitud BatchUpdateFindings en función de lo siguiente:
 - El resultado incluye un campo específico.

- El resultado incluye un valor de campo específico.

Claves de condición

Estas son las claves de condición para restringir el acceso a BatchUpdateFindings.

Campo de ASFF

La clave de condición de un campo de ASFF es la siguiente:

```
securityhub:ASFFSyntaxPath/<fieldName>
```

Sustituya *<fieldName>* por el campo de ASFF. Al configurar el acceso a BatchUpdateFindings, incluya uno o más campos de ASFF específicos en su política de IAM en lugar de un campo de nivel principal. Por ejemplo, para restringir el acceso al campo Workflow.Status, debe incluir securityhub:ASFFSyntaxPath/Workflow.Status en su política en lugar del campo de nivel principal Workflow.

Cómo no permitir todas las actualizaciones de un campo

Para evitar que un usuario actualice un campo específico, utilice una condición como esta:

```
"Condition": {
    "Null": {
        "securityhub:ASFFSyntaxPath/<fieldName>": "false"
    }
}
```

Por ejemplo, la siguiente declaración indica que no se puede usar BatchUpdateFindings para actualizar el campo de resultados Workflow.Status.

```
{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
  "Action": "securityhub:BatchUpdateFindings",
  "Resource": "*",
  "Condition": {
    "Null": {
      "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
    }
  }
}
```

```
}
}
```

Cómo no permitir valores de campo específicos

Para evitar que un usuario establezca un campo en un valor específico, utilice una condición como esta:

```
"Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
    }
}
```

Por ejemplo, la siguiente declaración indica que no se puede usar BatchUpdateFindings para establecer Workflow.Status como SUPPRESSED.

```
{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
  "Action": "securityhub:BatchUpdateFindings",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
  }
}
```

También puede proporcionar una lista de valores que no están permitidos.

```
"Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
        "<fieldValue2>", "<fieldValuen>" ]
    }
}
```

Por ejemplo, la siguiente declaración indica que no se puede usar BatchUpdateFindings para establecer Workflow.Status como RESOLVED o SUPPRESSED.

```
{
```

```
{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
  "Action": "securityhub:BatchUpdateFindings",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "securityhub:ASFFSyntaxPath/Workflow.Status": [
        "RESOLVED",
        "NOTIFIED"
      ]
    }
  }
}
```

Revisión de los detalles y el historial de búsquedas en Security Hub (CSPM)

En AWS Security Hub Cloud Security Posture Management (CSPM), un hallazgo es un registro observable de un control de seguridad o una detección relacionada con la seguridad. Security Hub CSPM genera un hallazgo cuando completa una comprobación de seguridad de un control y cuando ingiere un hallazgo de un producto integrado Servicio de AWS o de terceros. Cada resultado incluye un historial de cambios y otros detalles, como una clasificación de gravedad e información sobre los recursos afectados.

Puede revisar el historial y otros detalles de los hallazgos individuales en la consola CSPM de Security Hub o mediante programación con la API CSPM de Security Hub o el AWS CLI

Para ayudarlo a agilizar el análisis, la consola CSPM de Security Hub muestra un panel de búsqueda cuando elige un hallazgo específico. El panel incluye diferentes menús y pestañas para revisar los detalles específicos de un hallazgo.

Menús de acciones

Desde este menú, puede revisar el JSON completo de un resultado o agregar notas. A un hallazgo solo se le puede adjuntar una nota cada vez. Este menú también ofrece opciones para [configurar el estado del flujo de trabajo de una búsqueda](#) o [enviar una búsqueda a una acción personalizada](#) en Amazon EventBridge.

Menú de investigación

Desde este menú, puede investigar un resultado en Amazon Detective. Detective extrae entidades, como direcciones IP y AWS usuarios, de un hallazgo y visualiza su actividad. Puede

utilizar la actividad de la entidad como punto de partida para investigar la causa y el impacto de un resultado.

Pestaña Overview (Información general)

Esta pestaña proporciona un resumen de un hallazgo. Por ejemplo, puede determinar cuándo se creó y actualizó por última vez un hallazgo, en qué cuenta existe y el origen del hallazgo. Para los hallazgos de control, esta pestaña también muestra el nombre de la AWS Config regla asociada y un enlace a la guía de corrección en la documentación de CSPM de Security Hub.

En la instantánea de los recursos de la pestaña Descripción general, puede obtener una breve descripción de los recursos que intervienen en un hallazgo. En el caso de algunos recursos, se incluye la opción Abrir recurso, que enlaza directamente con el recurso afectado en la Servicio de AWS consola correspondiente. La instantánea del Historial muestra hasta dos cambios realizados en el resultado en la fecha más reciente para la que se está rastreando el historial. Por ejemplo, si realizó un cambio ayer y otro hoy, la instantánea mostrará el cambio de hoy. Para revisar las entradas anteriores, vaya a la pestaña Historial.

La fila Conformidad se expande para mostrar más detalles. Por ejemplo, si un control incluye parámetros, puede revisar los valores de los parámetros que Security Hub CSPM utiliza actualmente al realizar comprobaciones de seguridad para el control.

Pestaña recursos

En esta pestaña se proporcionan detalles sobre los recursos que intervienen en un resultado. Si ha iniciado sesión en la cuenta propietaria de un recurso, puede revisar el recurso en la consola correspondiente Servicio de AWS . Si no eres el propietario de un recurso, en esta pestaña se muestra el Cuenta de AWS ID del propietario.

La fila Detalles muestra los detalles específicos del recurso en un hallazgo. Muestra la [ResourceDetails](#) sección del hallazgo en formato JSON.

La fila Etiquetas muestra las claves y los valores de las etiquetas que se asignan a los recursos involucrados en un hallazgo. Los recursos que son [compatibles con la operación GetResources](#) de la API de etiquetado de AWS Resource Groups se pueden etiquetar. Security Hub CSPM llama a esta operación mediante un [rol vinculado a un servicio](#) cuando procesa hallazgos nuevos o actualizados, y recupera las etiquetas de recursos si el campo AWS Security Finding Format (ASFF) Resource . Id se rellena con el ARN de un recurso. Security Hub CSPM ignora el recurso no válido. IDs Para obtener más información sobre la inclusión de etiquetas de recursos en los resultados, consulte [Etiquetas](#).

Pestaña Historial

Esta pestaña rastrea el historial de un hallazgo. El historial de resultados está disponible para los resultados activos y archivados. Proporciona un registro inmutable de los cambios realizados en un hallazgo a lo largo del tiempo, incluyendo qué campo ASFF ha cambiado, cuándo se ha producido el cambio y qué usuario lo ha hecho. Cada página de la pestaña muestra hasta 20 cambios. Los cambios más recientes se muestran primero.

En el caso de los hallazgos activos, el historial de búsquedas está disponible durante un máximo de 90 días. En el caso de los hallazgos archivados, el historial de búsquedas está disponible durante un máximo de 30 días. El historial de búsquedas incluye los cambios que se realizaron de forma manual o automática mediante las reglas de [automatización CSPM de Security Hub](#). No incluye los cambios en los campos de fecha y hora de nivel superior, como los campos `CreatedAt` y `UpdatedAt`.

Si ha iniciado sesión en una cuenta de administrador CSPM de Security Hub, la búsqueda del historial corresponde a la cuenta de administrador y a todas las cuentas de los miembros.

Pestaña de amenazas

Esta pestaña incluye datos de los objetos [Action](#), [Malware](#) y [ProcessDetails](#) del ASFF, incluidos el tipo de amenaza y si un recurso es el objetivo o el actor. Por lo general, estos detalles se aplican a los hallazgos que se originan en Amazon GuardDuty.

Pestaña de vulnerabilidades

Esta pestaña muestra los datos del objeto [Vulnerability](#) del ASFF, incluyendo si hay vulnerabilidades o correcciones disponibles asociadas a un resultado. Estos detalles suelen aplicarse a las conclusiones que se originan en Amazon Inspector.

Las filas de cada pestaña incluyen una opción de copiar o filtrar. Por ejemplo, si abre el panel de un hallazgo cuyo estado de flujo de trabajo es Notificado, puede elegir la opción de filtro situada junto a la fila de estado del flujo de trabajo. Si elige Mostrar todos los hallazgos con este valor, Security Hub CSPM filtra la tabla de hallazgos y muestra solo los hallazgos con el mismo estado de flujo de trabajo.

Revisión de los detalles y el historial de resultados

Elija el método que prefiera y siga los pasos para revisar los detalles de búsqueda en Security Hub CSPM.

Si activó la agregación entre regiones e inicia sesión en la región de agregación, los datos de resultados incluyen datos de la región de agregación y de las regiones vinculadas. En otras regiones, los datos de resultados son específicos únicamente de esa región. Para obtener más información sobre la agregación entre regiones, consulte [Agregación de datos del CSPM en todas las regiones](#).

Security Hub CSPM console

Revisión de los detalles y el historial de resultados

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
2. Para mostrar una lista de resultado, realice una de las acciones siguientes:
 - En el panel de navegación, seleccione Resultados. Añada los filtros de búsqueda necesarios para reducir la lista de búsquedas.
 - En el panel de navegación, elija Insights. Elija una información. A continuación, en la lista de resultados, selecciona un resultado informativo.
 - En el panel de navegación, elija Integraciones. Seleccione Ver los resultados de una integración.
 - En el panel de navegación, elija Controles.
3. Elija un hallazgo. El panel de búsqueda muestra los detalles de la búsqueda.
4. En el panel de búsqueda, realice una de las siguientes acciones:
 - Para revisar los detalles específicos del hallazgo, selecciona una pestaña.
 - Para realizar una acción en relación con el hallazgo, elija una opción del menú Acciones.
 - Para investigar el hallazgo en Amazon Detective, selecciona la opción Investigar.

Note

Si te integras con una cuenta de miembro AWS Organizations y has iniciado sesión en ella, el panel de búsqueda incluirá el nombre de la cuenta. Para las cuentas de miembros que se invitan manualmente, en lugar de hacerlo a través de Organizations, el panel de búsqueda incluye solo el ID de la cuenta.

Security Hub CSPM API

Utilice la [GetFindings](#) operación de la API CSPM de Security Hub o, si está utilizando la AWS CLI, ejecute el [get-findings](#) comando. Puede proporcionar uno o más valores para el `Filters` parámetro a fin de limitar los resultados que desee recuperar.

Si el volumen de resultados es demasiado grande, puede utilizar el parámetro `MaxResults` para limitar los resultados a un número específico y el parámetro `NextToken` para paginar los resultados. Use el parámetro `SortCriteria` para ordenar los resultados por un campo específico.

Por ejemplo, el siguiente AWS CLI comando recupera los resultados que coinciden con los criterios de filtro especificados y ordena los resultados en orden descendente por campo. `LastObservedAt` Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (`\`) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub get-findings \
--filters '{"GeneratorId":[{"Value": "aws-
foundational","Comparison":"PREFIX"}],"WorkflowStatus": [{"Value":
"NEW","Comparison":"EQUALS"}],"Confidence": [{"Gte": 85}]}' --sort-criteria
'{"Field": "LastObservedAt","SortOrder": "desc"}' --page-size 5 --max-items 100
```

Para revisar el historial de resultados, utilice la operación [GetFindingHistory](#). Si está utilizando el AWS CLI, ejecute el [get-finding-history](#) comando. Identifique el resultado del que desea obtener un historial con los campos `ProductArn` y `Id`. Para obtener información acerca de estos campos, consulte [AwsSecurityFindingIdentifier](#). Cada solicitud puede recuperar el historial de un solo hallazgo.

Por ejemplo, el siguiente AWS CLI comando recupera el historial del hallazgo especificado. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (`\`) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub get-finding-history \
--region us-west-2 \
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-
EXAMPLE1111",ProductArn="arn:aws:securityhub:us-
west-2:123456789012:product/123456789012/default" \
--max-results 2 \
--start-time "2021-09-30T15:53:35.573Z" \
--end-time "2021-09-31T15:53:35.573Z"
```

PowerShell

Utilice el cmdlet `Get-SHUBFinding`. Si lo desea, rellene el `Filter` parámetro para limitar los resultados que desee recuperar.

Por ejemplo, el siguiente cmdlet recupera los resultados que coinciden con los filtros especificados.

```
Get-SHUBFinding -Filter @{AwsAccountId =  
  [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =  
  "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =  
  "EQUALS"; Value = 'FAILED'}}
```

Note

Si filtra las conclusiones por `CompanyName` o `ProductName`, el CSPM de Security Hub utiliza los valores que forman parte del objeto `ProductFields ASFF`. Security Hub CSPM no usa el nivel superior y los campos `CompanyName`. `ProductName`

Filtrado de resultados en Security Hub (CSPM)

AWS Security Hub Cloud Security Posture Management (CSPM) genera sus propios hallazgos a partir de los controles de seguridad y recibe los hallazgos de los productos integrados. Puede mostrar una lista de los resultados en las páginas Hallazgos, Integraciones e Información de la consola CSPM de Security Hub. Puede añadir filtros para reducir la lista de resultados de forma que sea relevante para su organización o caso de uso.

Para obtener información sobre cómo filtrar los resultados de un control de seguridad específico, consulte [the section called “Filtrado y clasificación de resultados de control”](#). La información de esta página se aplica a las páginas de hallazgos, perspectivas e integraciones.

Filtros predeterminados en las listas de búsqueda

De forma predeterminada, las listas de búsqueda en la consola CSPM de Security Hub se filtran en función de los `Workflow.Status` campos `RecordState` y del Formato de búsqueda de AWS seguridad (ASFF). Esto se suma a los filtros para obtener información o integración específicas.

El estado de registro indica si el resultado está activo o archivado. De forma predeterminada, las listas de hallazgos solo muestran los hallazgos activos. Un proveedor de resultados puede archivar un resultado si ya no está activo o no es importante. Security Hub CSPM también archiva automáticamente las conclusiones de control si se elimina el recurso asociado.

El estado de flujo de trabajo indica el estado de una investigación sobre un resultado. De forma predeterminada, las listas de hallazgos solo muestran los hallazgos con estado de flujo de trabajo NEW o NOTIFIED. Puede actualizar el estado de flujo de trabajo de un resultado.

Instrucciones para añadir filtros

Puede filtrar una lista de búsqueda por hasta diez atributos. Para cada atributo, puede proporcionar hasta 20 valores de filtro.

Al filtrar la lista de búsqueda, Security Hub CSPM aplica la AND lógica al conjunto de filtros. Un resultado solo coincide si coincide con todos los filtros proporcionados. Por ejemplo, si agrega GuardDuty un filtro para el nombre del producto y AwsS3Bucket un filtro para el tipo de recurso, Security Hub CSPM mostrará los resultados que coincidan con estos dos criterios.

Security Hub CSPM aplica la OR lógica a los filtros que utilizan el mismo atributo pero valores diferentes. Por ejemplo, si añade Amazon Inspector como valores de filtro para el nombre del producto, Security Hub CSPM mostrará las conclusiones generadas por Amazon Inspector GuardDuty o por cualquiera de ellas. GuardDuty

Para añadir filtros a una lista de resultados (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. Para mostrar una lista de resultados, realice una de las siguientes acciones desde el panel de navegación:
 - Elija Hallazgos.
 - Elija Información. Elija una información. A continuación, en la lista de resultados, elija un resultado prospectivo.
 - Seleccione Integraciones. Seleccione Ver los resultados de una integración.
3. En el cuadro Añadir filtros, selecciona uno o más archivos por los que filtrar.

Al filtrar por nombre de empresa o nombre de producto, la consola utiliza el nivel superior `CompanyName` y `ProductName` los campos del formato de búsqueda de AWS seguridad (ASFF). La API usa los valores que se encuentran debajo. `ProductFields`

4. Elija el tipo de coincidencia de filtro.

Para un filtro de cadenas, puedes elegir entre las siguientes opciones:

- es: busca un valor que coincida exactamente con el valor del filtro.
- empieza por: busca un valor que empiece por el valor del filtro.
- no es: busca un valor que no coincida con el valor del filtro.
- no empieza por: busca un valor que no empiece por el valor del filtro.

Para el campo Etiquetas de recursos, puede filtrar en función de claves o valores específicos.

Para un filtro numérico, puede elegir si desea proporcionar un solo número (Simple) o un rango de números (Range).

Para un filtro de fecha y hora, puede elegir si desea proporcionar un período de tiempo a partir de la fecha y hora actuales (Rolling window) o de un intervalo de fechas específico (Fixed range).

La adición de varios filtros tiene las siguientes interacciones:

- Los filtros es y empieza por van unidos por O. Un valor coincide si contiene alguno de los valores del filtro. Por ejemplo, si especifica que la Etiqueta de gravedad es CRÍTICA y la Etiqueta de gravedad es ALTA, los resultados incluyen tanto los resultados de gravedad crítica como de gravedad alta.
- Los filtros no es y no empieza por van unidos por AND. Un valor solo coincide si no contiene ninguno de esos valores de filtro. Por ejemplo, si especifica que la Etiqueta de gravedad no es BAJA y la Etiqueta de gravedad no es MEDIA, los resultados no incluyen los resultados de gravedad baja o media.

Si tiene un filtro es en un campo, no puede tener un filtro no es o no empieza por en el mismo campo.

5. Especifique el valor del filtro. Para los filtros de cadena, el valor del filtro distingue entre mayúsculas y minúsculas.

6. Seleccione Aplicar.

En el caso de un filtro existente, puede cambiar el tipo o el valor de la coincidencia del filtro. En una lista de resultados filtrada, elija el filtro. En el cuadro Editar filtro, elija el nuevo tipo o valor de coincidencia y, a continuación, seleccione Aplicar.

Para quitar un filtro, elija el icono x. La lista se actualiza automáticamente para reflejar el cambio.

Agrupación de hallazgos en Security Hub (CSPM)

Puede agrupar las conclusiones en AWS Security Hub Cloud Security Posture Management (CSPM) en función de los valores de un atributo seleccionado.

Al agrupar los resultados, la lista de resultados se reemplaza por una lista de valores para el atributo seleccionado en los resultados coincidentes. Para cada valor, la lista muestra el número de resultados coincidentes.

Por ejemplo, si agrupa los resultados por Cuenta de AWS identificador, verá una lista de identificadores de cuenta con el número de resultados coincidentes de cada cuenta.

Security Hub CSPM puede mostrar hasta 100 valores para un atributo seleccionado. Si hay más de 100 valores, solo verá los primeros 100.

Al elegir un valor de atributo, Security Hub CSPM muestra la lista de resultados coincidentes para ese valor.

Para agrupar los resultados en una lista de resultados (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. Para mostrar una lista de resultados, realice una de las siguientes acciones desde el panel de navegación:
 - Elija Hallazgos.
 - Elija Información. Elija una información. A continuación, en la lista de resultados, elija un resultado prospectivo.
 - Seleccione Integraciones. Seleccione Ver los resultados de una integración.
3. En la lista desplegable Agrupar por, elija el atributo que desea utilizar para la agrupación.

Para eliminar un atributo de agrupación, elija el icono x. Al eliminar el atributo de agrupación, la lista pasa de ser la lista de valores de atributo a ser una lista de resultados.

Configuración del estado del flujo de trabajo de los hallazgos en Security Hub (CSPM)

El estado de flujo de trabajo realiza un seguimiento del progreso de la investigación sobre un resultado. El estado del flujo de trabajo es específico de cada hallazgo individual y no afecta a la generación de nuevos hallazgos. Por ejemplo, si cambias el estado del flujo de trabajo de un hallazgo a SUPPRESSED o RESOLVED, tu cambio no impide que Security Hub CSPM genere un nuevo hallazgo para el mismo problema.

El estado del flujo de trabajo de un hallazgo puede ser uno de los siguientes valores.

¿NUEVO

Es el estado inicial de un resultado antes de revisarlo.

Los hallazgos que se ingieren de forma integrada Servicios de AWS, por ejemplo AWS Config, tienen NEW como estado inicial.

Security Hub CSPM también restablece el estado del flujo de trabajo desde NOTIFIED o RESOLVED hasta NEW en los siguientes casos:

- `RecordState` cambia de ARCHIVED a ACTIVE.
- `Compliance.Status` cambia de PASSED a FAILED, WARNING o NOT_AVAILABLE.

Estos cambios implican que es necesaria una investigación adicional.

NOTIFICADO

Indica que informé sobre el problema de seguridad al propietario del recurso. Puede utilizar este estado cuando no sea el propietario del recurso y necesite la intervención del propietario para que se resuelva un problema de seguridad.

Si se produce una de las siguientes situaciones, el estado del flujo de trabajo cambia automáticamente de NOTIFIED a NEW:

- `RecordState` cambia de ARCHIVED a ACTIVE.
- `Compliance.Status` cambia de PASSED a FAILED, WARNING o NOT_AVAILABLE.

SUPRIMIDO

Indica que ha revisado el resultado y no cree que sea necesario realizar ninguna acción.

El estado del flujo de trabajo de un resultado del tipo SUPPRESSED no cambia si RecordState cambia de ARCHIVED a ACTIVE.

RESUELTO

El hallazgo se ha revisado y se ha corregido. Ahora se considera resuelto.

El resultado permanece como RESOLVED a menos que se produzca alguna de las siguientes situaciones:

- RecordState cambia de ARCHIVED a ACTIVE.
- Compliance.Status cambia de PASSED a FAILED, WARNING o NOT_AVAILABLE.

En esos casos, el estado del flujo de trabajo se restablece automáticamente a NEW.

En el caso de los hallazgos de los controles, si Compliance.Status es PASSED así, Security Hub CSPM establece automáticamente el estado del flujo de trabajo en. RESOLVED

Configuración del estado de flujo de trabajo de los resultados

Para cambiar el estado del flujo de trabajo de uno o más hallazgos, puede utilizar la consola CSPM de Security Hub o la API CSPM de Security Hub. Si cambias el estado del flujo de trabajo de un hallazgo, ten en cuenta que Security Hub CSPM puede tardar varios minutos en procesar tu solicitud y actualizar el hallazgo.

Tip

También puede cambiar el estado del flujo de trabajo de los hallazgos automáticamente mediante reglas de automatización. Con las reglas de automatización, se configura Security Hub CSPM para que actualice automáticamente el estado del flujo de trabajo de los hallazgos en función de los criterios que especifique. Para obtener más información, consulte [Descripción de las reglas de automatización en Security Hub CSPM](#).

Para cambiar el estado del flujo de trabajo de uno o más hallazgos, elija el método que prefiera y siga los pasos.

Security Hub CSPM console

Para cambiar el estado del flujo de trabajo de los hallazgos

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, realice una de las siguientes acciones para mostrar una tabla de resultados:
 - Elija Hallazgos.
 - Elija Información. A continuación, elija una idea. En los resultados de la información, elija un resultado.
 - Seleccione Integraciones. A continuación, en la sección de integración, selecciona Ver resultados.
 - Elige Estándares de seguridad. A continuación, en la sección correspondiente a la norma, selecciona Ver resultados. En la tabla de controles, elija un control para mostrar los resultados del control.
3. En la tabla de hallazgos, active la casilla de verificación de cada búsqueda cuyo estado de flujo de trabajo desee cambiar.
4. En la parte superior de la página, elija el estado del flujo de trabajo y, a continuación, elija el nuevo estado del flujo de trabajo para los hallazgos seleccionados.
5. En el cuadro de diálogo Definir el estado del flujo de trabajo, si lo desea, introduzca una nota que detalle el motivo del cambio del estado del flujo de trabajo. A continuación, elija Establecer estado.

Security Hub CSPM API

Utilice la operación [BatchUpdateFindings](#). Proporcione el ID de resultado y el ARN del producto que generó el resultado. Puede obtener estos detalles mediante la [GetFindings](#) operación.

AWS CLI

Ejecute el comando [batch-update-findings](#). Proporcione el ID de resultado y el ARN del producto que generó el resultado. Puede obtener estos detalles ejecutando el comando [get-findings](#).

```
batch-update-findings --finding-identifiers  
Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

Ejemplo

```
aws securityhub batch-update-findings --finding-identifiers
  Id="arn:aws:securityhub:us-west-1:123456789012:subscription/
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --
workflow Status="RESOLVED"
```

Enviar los resultados a un Security Hub (CSPM) personalizado (acción)

Puede crear acciones personalizadas AWS de Security Hub Cloud Security Posture Management (CSPM) para automatizar el Security Hub CSPM con Amazon. EventBridge Para las acciones personalizadas, el tipo de evento es Security Hub Findings - Custom Action. Después de configurar una acción personalizada, puede enviarle hallazgos. Para obtener más información y pasos detallados sobre cómo crear acciones personalizadas, consulte [the section called “Respuesta y corrección automatizadas”](#).

Cómo enviar resultados a una acción personalizada (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. Para mostrar una lista de resultado, realice una de las acciones siguientes:
 - En el panel de navegación CSPM de Security Hub, elija Hallazgos.
 - En el panel de navegación CSPM de Security Hub, elija Insights. Elija una información. A continuación, en la lista de resultados, seleccione un resultado de información.
 - En el panel de navegación CSPM de Security Hub, elija Integraciones. Seleccione Ver los resultados de una integración.
 - En el panel de navegación CSPM de Security Hub, elija Estándares de seguridad. Seleccione Ver resultados para ver una lista de controles. A continuación, elija el nombre del control.
3. En la lista de resultados, seleccione la casilla de verificación de cada resultado que desee enviar a la acción personalizada.

Puede seleccionar hasta 20 hallazgos a la vez.

4. En Acciones, elija la acción personalizada.

AWS Formato de búsqueda de seguridad (ASFF)

AWS Security Hub Cloud Security Posture Management (CSPM) consume y agrega los hallazgos de productos integrados Servicios de AWS y de terceros. Security Hub CSPM procesa estos hallazgos mediante un formato de hallazgos estándar denominado AWS Security Finding Format (ASFF), que elimina la necesidad de realizar esfuerzos de conversión de datos que consumen mucho tiempo.

Esta página proporciona un resumen completo del JSON para realizar una búsqueda en el formato de búsqueda de AWS seguridad (ASFF). El formato se deriva del esquema [JSON](#). Elija el nombre de un objeto vinculado para revisar un ejemplo de un hallazgo de ese objeto. Comparar las conclusiones del CSPM de Security Hub con los recursos y ejemplos que se muestran aquí puede ayudarle a interpretar las conclusiones.

Para obtener descripciones de los atributos individuales del ASFF, consulte y. [the section called “Atributos de nivel superior necesarios del ASFF”](#) [the section called “Atributos de nivel superior opcionales del ASFF”](#)

```
"Findings": [  
  {  
    "Action": {  
      "ActionType": "string",  
      "AwsApiCallAction": {  
        "AffectedResources": {  
          "string": "string"  
        },  
        "Api": "string",  
        "CallerType": "string",  
        "DomainDetails": {  
          "Domain": "string"  
        },  
        "FirstSeen": "string",  
        "LastSeen": "string",  
        "RemoteIpDetails": {  
          "City": {  
            "CityName": "string"  
          },  
          "Country": {  
            "CountryCode": "string",  
            "CountryName": "string"  
          },  
          "IpAddressV4": "string",  
          "Geolocation": {
```

```
    "Lat": number,
    "Lon": number
  },
  "Organization": {
    "Asn": number,
    "AsnOrg": "string",
    "Isp": "string",
    "Org": "string"
  }
},
"ServiceName": "string"
},
"DnsRequestAction": {
  "Blocked": boolean,
  "Domain": "string",
  "Protocol": "string"
},
"NetworkConnectionAction": {
  "Blocked": boolean,
  "ConnectionDirection": "string",
  "LocalPortDetails": {
    "Port": number,
    "PortName": "string"
  },
  "Protocol": "string",
  "RemoteIpDetails": {
    "City": {
      "CityName": "string"
    },
    "Country": {
      "CountryCode": "string",
      "CountryName": "string"
    },
    "IpAddressV4": "string",
    "Geolocation": {
      "Lat": number,
      "Lon": number
    },
    "Organization": {
      "Asn": number,
      "AsnOrg": "string",
      "Isp": "string",
      "Org": "string"
    }
  }
}
```

```

    },
    "RemotePortDetails": {
      "Port": number,
      "PortName": "string"
    }
  },
  "PortProbeAction": {
    "Blocked": boolean,
    "PortProbeDetails": [{
      "LocalIpDetails": {
        "IpAddressV4": "string"
      },
      "LocalPortDetails": {
        "Port": number,
        "PortName": "string"
      },
      "RemoteIpDetails": {
        "City": {
          "CityName": "string"
        },
        "Country": {
          "CountryCode": "string",
          "CountryName": "string"
        },
        "GeoLocation": {
          "Lat": number,
          "Lon": number
        },
        "IpAddressV4": "string",
        "Organization": {
          "Asn": number,
          "AsnOrg": "string",
          "Isp": "string",
          "Org": "string"
        }
      }
    ]
  },
  "AwsAccountId": "string",
  "AwsAccountName": "string",
  "CompanyName": "string",
  "Compliance": {
    "AssociatedStandards": [{

```

```

    "StandardsId": "string"
  }],
  "RelatedRequirements": ["string"],
  "SecurityControlId": "string",
  "SecurityControlParameters": [
    {
      "Name": "string",
      "Value": ["string"]
    }
  ],
  "Status": "string",
  "StatusReasons": [
    {
      "Description": "string",
      "ReasonCode": "string"
    }
  ]
},
"Confidence": number,
"CreatedAt": "string",
"Criticality": number,
"Description": "string",
"Detection": {
  "Sequence": {
    "Uid": "string",
    "Actors": [{
      "Id": "string",
      "Session": {
        "Uid": "string",
        "MfaStatus": "string",
        "CreatedTime": "string",
        "Issuer": "string"
      }
    }],
    "User": {
      "CredentialUid": "string",
      "Name": "string",
      "Type": "string",
      "Uid": "string",
      "Account": {
        "Uid": "string",
        "Name": "string"
      }
    }
  }
}],

```

```
"Endpoints": [{
  "Id": "string",
  "Ip": "string",
  "Domain": "string",
  "Port": number,
  "Location": {
    "City": "string",
    "Country": "string",
    "Lat": number,
    "Lon": number
  },
  "AutonomousSystem": {
    "Name": "string",
    "Number": number
  },
  "Connection": {
    "Direction": "string"
  }
}],
"Signals": [{
  "Id": "string",
  "Title": "string",
  "ActorIds": ["string"],
  "Count": number,
  "FirstSeenAt": number,
  "SignalIndicators": [
    {
      "Key": "string",
      "Title": "string",
      "Values": ["string"]
    },
    {
      "Key": "string",
      "Title": "string",
      "Values": ["string"]
    }
  ],
  "LastSeenAt": number,
  "Name": "string",
  "ResourceIds": ["string"],
  "Type": "string"
}],
"SequenceIndicators": [
  {
```

```

    "Key": "string",
    "Title": "string",
    "Values": ["string"]
  },
  {
    "Key": "string",
    "Title": "string",
    "Values": ["string"]
  }
]
}
},
"FindingProviderFields": {
  "Confidence": number,
  "Criticality": number,
  "RelatedFindings": [{
    "ProductArn": "string",
    "Id": "string"
  }],
  "Severity": {
    "Label": "string",
    "Normalized": number,
    "Original": "string"
  },
  "Types": ["string"]
},
"FirstObservedAt": "string",
"GeneratorId": "string",
"Id": "string",
"LastObservedAt": "string",
"Malware": [{
  "Name": "string",
  "Path": "string",
  "State": "string",
  "Type": "string"
}],
"Network": {
  "DestinationDomain": "string",
  "DestinationIPv4": "string",
  "DestinationIPv6": "string",
  "DestinationPort": number,
  "Direction": "string",
  "OpenPortRange": {
    "Begin": integer,

```



```
    "End": integer
  },
  "Protocol": "string",
  "SourceDomain": "string",
  "SourceIPv4": "string",
  "SourceIPv6": "string",
  "SourceMac": "string",
  "SourcePort": number
},
"NetworkPath": [{
  "ComponentId": "string",
  "ComponentType": "string",
  "Egress": {
    "Destination": {
      "Address": ["string"],
      "PortRanges": [{
        "Begin": integer,
        "End": integer
      }]
    },
    "Protocol": "string",
    "Source": {
      "Address": ["string"],
      "PortRanges": [{
        "Begin": integer,
        "End": integer
      }]
    }
  },
  "Ingress": {
    "Destination": {
      "Address": ["string"],
      "PortRanges": [{
        "Begin": integer,
        "End": integer
      }]
    },
    "Protocol": "string",
    "Source": {
      "Address": ["string"],
      "PortRanges": [{
        "Begin": integer,
        "End": integer
      }]
    }
  }
}]
```

```

    }
  }
}],
  "Note": {
    "Text": "string",
    "UpdatedAt": "string",
    "UpdatedBy": "string"
  },
  "PatchSummary": {
    "FailedCount": number,
    "Id": "string",
    "InstalledCount": number,
    "InstalledOtherCount": number,
    "InstalledPendingReboot": number,
    "InstalledRejectedCount": number,
    "MissingCount": number,
    "Operation": "string",
    "OperationEndTime": "string",
    "OperationStartTime": "string",
    "RebootOption": "string"
  },
  "Process": {
    "LaunchedAt": "string",
    "Name": "string",
    "ParentPid": number,
    "Path": "string",
    "Pid": number,
    "TerminatedAt": "string"
  },
  "ProductArn": "string",
  "ProductFields": {
    "string": "string"
  },
  "ProductName": "string",
  "RecordState": "string",
  "Region": "string",
  "RelatedFindings": [{
    "Id": "string",
    "ProductArn": "string"
  }],
  "Remediation": {
    "Recommendation": {
      "Text": "string",
      "Url": "string"
    }
  }
}
```

```
}
},
"Resources": [{
  "ApplicationArn": "string",
  "ApplicationName": "string",
  "DataClassification": {
    "DetailedResultsLocation": "string",
    "Result": {
      "AdditionalOccurrences": boolean,
      "CustomDataIdentifiers": {
        "Detections": [{
          "Arn": "string",
          "Count": integer,
          "Name": "string",
          "Occurrences": {
            "Cells": [{
              "CellReference": "string",
              "Column": integer,
              "ColumnName": "string",
              "Row": integer
            }],
            "LineRanges": [{
              "End": integer,
              "Start": integer,
              "StartColumn": integer
            }],
            "OffsetRanges": [{
              "End": integer,
              "Start": integer,
              "StartColumn": integer
            }],
            "Pages": [{
              "LineRange": {
                "End": integer,
                "Start": integer,
                "StartColumn": integer
              },
              "OffsetRange": {
                "End": integer,
                "Start": integer,
                "StartColumn": integer
              },
              "PageNumber": integer
            }],

```

```
    "Records": [{
      "JsonPath": "string",
      "RecordIndex": integer
    }]
  },
  "TotalCount": integer
},
"MimeType": "string",
"SensitiveData": [{
  "Category": "string",
  "Detections": [{
    "Count": integer,
    "Occurrences": {
      "Cells": [{
        "CellReference": "string",
        "Column": integer,
        "ColumnName": "string",
        "Row": integer
      }],
      "LineRanges": [{
        "End": integer,
        "Start": integer,
        "StartColumn": integer
      }],
      "OffsetRanges": [{
        "End": integer,
        "Start": integer,
        "StartColumn": integer
      }],
      "Pages": [{
        "LineRange": {
          "End": integer,
          "Start": integer,
          "StartColumn": integer
        },
        "OffsetRange": {
          "End": integer,
          "Start": integer,
          "StartColumn": integer
        },
        "PageNumber": integer
      }],
      "Records": [{
```

```

        "JsonPath": "string",
        "RecordIndex": integer
    }],
    "Type": "string"
}],
    "TotalCount": integer
}],
    "SizeClassified": integer,
    "Status": {
        "Code": "string",
        "Reason": "string"
    }
}
},
"Details": {
    "AwsAmazonMQBroker": {
        "AutoMinorVersionUpgrade": boolean,
        "BrokerArn": "string",
        "BrokerId": "string",
        "BrokerName": "string",
        "Configuration": {
            "Id": "string",
            "Revision": integer
        },
        "DeploymentMode": "string",
        "EncryptionOptions": {
            "UseAwsOwnedKey": boolean
        },
        "EngineType": "string",
        "EngineVersion": "string",
        "HostInstanceType": "string",
        "Logs": {
            "Audit": boolean,
            "AuditLogGroup": "string",
            "General": boolean,
            "GeneralLogGroup": "string"
        },
        "MaintenanceWindowStartTime": {
            "DayOfWeek": "string",
            "TimeOfDay": "string",
            "TimeZone": "string"
        },
        "PubliclyAccessible": boolean,

```

```

    "SecurityGroups": [
      "string"
    ],
    "StorageType": "string",
    "SubnetIds": [
      "string",
      "string"
    ],
    "Users": [{
      "Username": "string"
    }]
  },
  "AwsApiGatewayRestApi": {
    "ApiKeySource": "string",
    "BinaryMediaTypes": [" string"],
    "CreatedDate": "string",
    "Description": "string",
    "EndpointConfiguration": {
      "Types": ["string"]
    },
    "Id": "string",
    "MinimumCompressionSize": number,
    "Name": "string",
    "Version": "string"
  },
  "AwsApiGatewayStage": {
    "AccessLogSettings": {
      "DestinationArn": "string",
      "Format": "string"
    },
    "CacheClusterEnabled": boolean,
    "CacheClusterSize": "string",
    "CacheClusterStatus": "string",
    "CanarySettings": {
      "DeploymentId": "string",
      "PercentTraffic": number,
      "StageVariableOverrides": [{
        "string": "string"
      }],
      "UseStageCache": boolean
    },
    "ClientCertificateId": "string",
    "CreatedDate": "string",
    "DeploymentId": "string",

```

```

    "Description": "string",
    "DocumentationVersion": "string",
    "LastUpdatedDate": "string",
    "MethodSettings": [{
      "CacheDataEncrypted": boolean,
      "CachingEnabled": boolean,
      "CacheTtlInSeconds": number,
      "DataTraceEnabled": boolean,
      "HttpMethod": "string",
      "LoggingLevel": "string",
      "MetricsEnabled": boolean,
      "RequireAuthorizationForCacheControl": boolean,
      "ResourcePath": "string",
      "ThrottlingBurstLimit": number,
      "ThrottlingRateLimit": number,
      "UnauthorizedCacheControlHeaderStrategy": "string"
    }],
    "StageName": "string",
    "TracingEnabled": boolean,
    "Variables": {
      "string": "string"
    },
    "WebAclArn": "string"
  },
  "AwsApiGatewayV2Api": {
    "ApiEndpoint": "string",
    "ApiId": "string",
    "ApiKeySelectionExpression": "string",
    "CorsConfiguration": {
      "AllowCredentials": boolean,
      "AllowHeaders": ["string"],
      "AllowMethods": ["string"],
      "AllowOrigins": ["string"],
      "ExposeHeaders": ["string"],
      "MaxAge": number
    },
    "CreatedDate": "string",
    "Description": "string",
    "Name": "string",
    "ProtocolType": "string",
    "RouteSelectionExpression": "string",
    "Version": "string"
  },
  "AwsApiGatewayV2Stage": {

```

```

"AccessLogSettings": {
  "DestinationArn": "string",
  "Format": "string"
},
"ApiGatewayManaged": boolean,
"AutoDeploy": boolean,
"ClientCertificateId": "string",
"CreateDate": "string",
"DefaultRouteSettings": {
  "DataTraceEnabled": boolean,
  "DetailedMetricsEnabled": boolean,
  "LoggingLevel": "string",
  "ThrottlingBurstLimit": number,
  "ThrottlingRateLimit": number
},
"DeploymentId": "string",
"Description": "string",
"LastDeploymentStatusMessage": "string",
"LastUpdatedDate": "string",
"RouteSettings": {
  "DetailedMetricsEnabled": boolean,
  "LoggingLevel": "string",
  "DataTraceEnabled": boolean,
  "ThrottlingBurstLimit": number,
  "ThrottlingRateLimit": number
},
"StageName": "string",
"StageVariables": [{
  "string": "string"
}]
},
"AwsAppSyncGraphQLApi": {
  "AwsAppSyncGraphQLApi": {
    "AdditionalAuthenticationProviders": [
      {
        "AuthenticationType": "string",
        "LambdaAuthorizerConfig": {
          "AuthorizerResultTtlInSeconds": integer,
          "AuthorizerUri": "string"
        }
      }
    ],
    {
      "AuthenticationType": "string"
    }
  }
}

```



```

    ],
    "ApiId": "string",
    "Arn": "string",
    "AuthenticationType": "string",
    "Id": "string",
    "LogConfig": {
      "CloudWatchLogsRoleArn": "string",
      "ExcludeVerboseContent": boolean,
      "FieldLogLevel": "string"
    },
    "Name": "string",
    "XrayEnabled": boolean
  }
},
"AwsAthenaWorkGroup": {
  "Description": "string",
  "Name": "string",
  "WorkgroupConfiguration": {
    "ResultConfiguration": {
      "EncryptionConfiguration": {
        "EncryptionOption": "string",
        "KmsKey": "string"
      }
    }
  },
  "State": "string"
},
"AwsAutoScalingAutoScalingGroup": {
  "AvailabilityZones": [{
    "Value": "string"
  }],
  "CreatedTime": "string",
  "HealthCheckGracePeriod": integer,
  "HealthCheckType": "string",
  "LaunchConfigurationName": "string",
  "LoadBalancerNames": ["string"],
  "LaunchTemplate": {
    "LaunchTemplateId": "string",
    "LaunchTemplateName": "string",
    "Version": "string"
  },
  "MixedInstancesPolicy": {
    "InstancesDistribution": {
      "OnDemandAllocationStrategy": "string",

```

```

    "OnDemandBaseCapacity": number,
    "OnDemandPercentageAboveBaseCapacity": number,
    "SpotAllocationStrategy": "string",
    "SpotInstancePools": number,
    "SpotMaxPrice": "string"
  },
  "LaunchTemplate": {
    "LaunchTemplateSpecification": {
      "LaunchTemplateId": "string",
      "LaunchTemplateName": "string",
      "Version": "string"
    },
    "CapacityRebalance": boolean,
    "Overrides": [{
      "InstanceType": "string",
      "WeightedCapacity": "string"
    }]
  }
}
},
"AwsAutoScalingLaunchConfiguration": {
  "AssociatePublicIpAddress": boolean,
  "BlockDeviceMappings": [{
    "DeviceName": "string",
    "Ebs": {
      "DeleteOnTermination": boolean,
      "Encrypted": boolean,
      "Iops": number,
      "SnapshotId": "string",
      "VolumeSize": number,
      "VolumeType": "string"
    },
    "NoDevice": boolean,
    "VirtualName": "string"
  }],
  "ClassicLinkVpcId": "string",
  "ClassicLinkVpcSecurityGroups": ["string"],
  "CreatedTime": "string",
  "EbsOptimized": boolean,
  "IamInstanceProfile": "string"
},
"ImageId": "string",
"InstanceMonitoring": {
  "Enabled": boolean

```

```

    },
    "InstanceType": "string",
    "KernelId": "string",
    "KeyName": "string",
    "LaunchConfigurationName": "string",
    "MetadataOptions": {
      "HttpEndPoint": "string",
      "HttpPutReponseHopLimit": number,
      "HttpTokens": "string"
    },
    "PlacementTenancy": "string",
    "RamdiskId": "string",
    "SecurityGroups": ["string"],
    "SpotPrice": "string",
    "UserData": "string"
  },
  "AwsBackupBackupPlan": {
    "BackupPlan": {
      "AdvancedBackupSettings": [{
        "BackupOptions": {
          "WindowsVSS": "string"
        },
        "ResourceType": "string"
      }],
      "BackupPlanName": "string",
      "BackupPlanRule": [{
        "CompletionWindowMinutes": integer,
        "CopyActions": [{
          "DestinationBackupVaultArn": "string",
          "Lifecycle": {
            "DeleteAfterDays": integer,
            "MoveToColdStorageAfterDays": integer
          }
        }],
        "Lifecycle": {
          "DeleteAfterDays": integer
        },
        "RuleName": "string",
        "ScheduleExpression": "string",
        "StartWindowMinutes": integer,
        "TargetBackupVault": "string"
      }]
    },
    "BackupPlanArn": "string",

```

```

    "BackupPlanId": "string",
    "VersionId": "string"
  },
  "AwsBackupBackupVault": {
    "AccessPolicy": {
      "Statement": [{
        "Action": ["string"],
        "Effect": "string",
        "Principal": {
          "AWS": "string"
        },
        "Resource": "string"
      }],
      "Version": "string"
    },
    "BackupVaultArn": "string",
    "BackupVaultName": "string",
    "EncryptionKeyArn": "string",
    "Notifications": {
      "BackupVaultEvents": ["string"],
      "SNSTopicArn": "string"
    }
  },
  "AwsBackupRecoveryPoint": {
    "BackupSizeInBytes": integer,
    "BackupVaultName": "string",
    "BackupVaultArn": "string",
    "CalculatedLifecycle": {
      "DeleteAt": "string",
      "MoveToColdStorageAt": "string"
    },
    "CompletionDate": "string",
    "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanVersion": "string",
      "BackupRuleId": "string"
    },
    "CreationDate": "string",
    "EncryptionKeyArn": "string",
    "IamRoleArn": "string",
    "IsEncrypted": boolean,
    "LastRestoreTime": "string",
    "Lifecycle": {

```

```

    "DeleteAfterDays": integer,
    "MoveToColdStorageAfterDays": integer
  },
  "RecoveryPointArn": "string",
  "ResourceArn": "string",
  "ResourceType": "string",
  "SourceBackupVaultArn": "string",
  "Status": "string",
  "StatusMessage": "string",
  "StorageClass": "string"
},
"AwsCertificateManagerCertificate": {
  "CertificateAuthorityArn": "string",
  "CreatedAt": "string",
  "DomainName": "string",
  "DomainValidationOptions": [{
    "DomainName": "string",
    "ResourceRecord": {
      "Name": "string",
      "Type": "string",
      "Value": "string"
    },
    "ValidationDomain": "string",
    "ValidationEmails": ["string"],
    "ValidationMethod": "string",
    "ValidationStatus": "string"
  }],
  "ExtendedKeyUsages": [{
    "Name": "string",
    "OId": "string"
  }],
  "FailureReason": "string",
  "ImportedAt": "string",
  "InUseBy": ["string"],
  "IssuedAt": "string",
  "Issuer": "string",
  "KeyAlgorithm": "string",
  "KeyUsages": [{
    "Name": "string"
  }],
  "NotAfter": "string",
  "NotBefore": "string",
  "Options": {
    "CertificateTransparencyLoggingPreference": "string"
  }
}

```

```

},
"RenewalEligibility": "string",
"RenewalSummary": {
  "DomainValidationOptions": [{
    "DomainName": "string",
    "ResourceRecord": {
      "Name": "string",
      "Type": "string",
      "Value": "string"
    },
    "ValidationDomain": "string",
    "ValidationEmails": ["string"],
    "ValidationMethod": "string",
    "ValidationStatus": "string"
  }],
  "RenewalStatus": "string",
  "RenewalStatusReason": "string",
  "UpdatedAt": "string"
},
"Serial": "string",
"SignatureAlgorithm": "string",
"Status": "string",
"Subject": "string",
"SubjectAlternativeNames": ["string"],
"Type": "string"
},
"AwsCloudFormationStack": {
  "Capabilities": ["string"],
  "CreationTime": "string",
  "Description": "string",
  "DisableRollback": boolean,
  "DriftInformation": {
    "StackDriftStatus": "string"
  },
  "EnableTerminationProtection": boolean,
  "LastUpdatedTime": "string",
  "NotificationArns": ["string"],
  "Outputs": [{
    "Description": "string",
    "OutputKey": "string",
    "OutputValue": "string"
  }],
  "RoleArn": "string",
  "StackId": "string",

```

```

    "StackName": "string",
    "StackStatus": "string",
    "StackStatusReason": "string",
    "TimeoutInMinutes": number
  },
  "AwsCloudFrontDistribution": {
    "CacheBehaviors": {
      "Items": [{
        "ViewerProtocolPolicy": "string"
      }]
    },
    "DefaultCacheBehavior": {
      "ViewerProtocolPolicy": "string"
    },
    "DefaultRootObject": "string",
    "DomainName": "string",
    "Etag": "string",
    "LastModifiedTime": "string",
    "Logging": {
      "Bucket": "string",
      "Enabled": boolean,
      "IncludeCookies": boolean,
      "Prefix": "string"
    },
    "OriginGroups": {
      "Items": [{
        "FailoverCriteria": {
          "StatusCodes": {
            "Items": [number],
            "Quantity": number
          }
        }
      }]
    },
    "Origins": {
      "Items": [{
        "CustomOriginConfig": {
          "HttpPort": number,
          "HttpsPort": number,
          "OriginKeepaliveTimeout": number,
          "OriginProtocolPolicy": "string",
          "OriginReadTimeout": number,
          "OriginSslProtocols": {
            "Items": ["string"],

```

```

        "Quantity": number
      }
    },
    "DomainName": "string",
    "Id": "string",
    "OriginPath": "string",
    "S3OriginConfig": {
      "OriginAccessIdentity": "string"
    }
  ]
},
"Status": "string",
"ViewerCertificate": {
  "AcmCertificateArn": "string",
  "Certificate": "string",
  "CertificateSource": "string",
  "CloudFrontDefaultCertificate": boolean,
  "IamCertificateId": "string",
  "MinimumProtocolVersion": "string",
  "SslSupportMethod": "string"
},
"WebAclId": "string"
},
"AwsCloudTrailTrail": {
  "CloudWatchLogsLogGroupArn": "string",
  "CloudWatchLogsRoleArn": "string",
  "HasCustomEventSelectors": boolean,
  "HomeRegion": "string",
  "IncludeGlobalServiceEvents": boolean,
  "IsMultiRegionTrail": boolean,
  "IsOrganizationTrail": boolean,
  "KmsKeyId": "string",
  "LogFileValidationEnabled": boolean,
  "Name": "string",
  "S3BucketName": "string",
  "S3KeyPrefix": "string",
  "SnsTopicArn": "string",
  "SnsTopicName": "string",
  "TrailArn": "string"
},
"AwsCloudWatchAlarm": {
  "ActionsEnabled": boolean,
  "AlarmActions": ["string"],
  "AlarmArn": "string",

```



```

    "AlarmConfigurationUpdatedTimestamp": "string",
    "AlarmDescription": "string",
    "AlarmName": "string",
    "ComparisonOperator": "string",
    "DatapointsToAlarm": number,
    "Dimensions": [{
      "Name": "string",
      "Value": "string"
    }],
    "EvaluateLowSampleCountPercentile": "string",
    "EvaluationPeriods": number,
    "ExtendedStatistic": "string",
    "InsufficientDataActions": ["string"],
    "MetricName": "string",
    "Namespace": "string",
    "OkActions": ["string"],
    "Period": number,
    "Statistic": "string",
    "Threshold": number,
    "ThresholdMetricId": "string",
    "TreatMissingData": "string",
    "Unit": "string"
  },
  "AwsCodeBuildProject": {
    "Artifacts": [{
      "ArtifactIdentifier": "string",
      "EncryptionDisabled": boolean,
      "Location": "string",
      "Name": "string",
      "NamespaceType": "string",
      "OverrideArtifactName": boolean,
      "Packaging": "string",
      "Path": "string",
      "Type": "string"
    }],
    "SecondaryArtifacts": [{
      "ArtifactIdentifier": "string",
      "Type": "string",
      "Location": "string",
      "Name": "string",
      "NamespaceType": "string",
      "Packaging": "string",
      "Path": "string",
      "EncryptionDisabled": boolean,

```

```

        "OverrideArtifactName": boolean
    }],
    "EncryptionKey": "string",
    "Certificate": "string",
    "Environment": {
        "Certificate": "string",
        "EnvironmentVariables": [{
            "Name": "string",
            "Type": "string",
            "Value": "string"
        }],
        "ImagePullCredentialsType": "string",
        "PrivilegedMode": boolean,
        "RegistryCredential": {
            "Credential": "string",
            "CredentialProvider": "string"
        },
        "Type": "string"
    },
    "LogsConfig": {
        "CloudWatchLogs": {
            "GroupName": "string",
            "Status": "string",
            "StreamName": "string"
        },
        "S3Logs": {
            "EncryptionDisabled": boolean,
            "Location": "string",
            "Status": "string"
        }
    },
    "Name": "string",
    "ServiceRole": "string",
    "Source": {
        "Type": "string",
        "Location": "string",
        "GitCloneDepth": integer
    },
    "VpcConfig": {
        "VpcId": "string",
        "Subnets": ["string"],
        "SecurityGroupIds": ["string"]
    }
},

```

```
"AwsDmsEndpoint": {
  "CertificateArn": "string",
  "DatabaseName": "string",
  "EndpointArn": "string",
  "EndpointIdentifier": "string",
  "EndpointType": "string",
  "EngineName": "string",
  "KmsKeyId": "string",
  "Port": integer,
  "ServerName": "string",
  "SslMode": "string",
  "Username": "string"
},
"AwsDmsReplicationInstance": {
  "AllocatedStorage": integer,
  "AutoMinorVersionUpgrade": boolean,
  "AvailabilityZone": "string",
  "EngineVersion": "string",
  "KmsKeyId": "string",
  "MultiAZ": boolean,
  "PreferredMaintenanceWindow": "string",
  "PubliclyAccessible": boolean,
  "ReplicationInstanceClass": "string",
  "ReplicationInstanceIdentifier": "string",
  "ReplicationSubnetGroup": {
    "ReplicationSubnetGroupIdentifier": "string"
  },
  "VpcSecurityGroups": [
    {
      "VpcSecurityGroupId": "string"
    }
  ]
},
"AwsDmsReplicationTask": {
  "CdcStartPosition": "string",
  "Id": "string",
  "MigrationType": "string",
  "ReplicationInstanceArn": "string",
  "ReplicationTaskIdentifier": "string",
  "ReplicationTaskSettings": {
    "string": "string"
  },
  "SourceEndpointArn": "string",
  "TableMappings": {
```

```
    "string": "string"
  },
  "TargetEndpointArn": "string"
},
"AwsDynamoDbTable": {
  "AttributeDefinitions": [{
    "AttributeName": "string",
    "AttributeType": "string"
  }],
  "BillingModeSummary": {
    "BillingMode": "string",
    "LastUpdateToPayPerRequestDateTime": "string"
  },
  "CreationDateTime": "string",
  "DeletionProtectionEnabled": boolean,
  "GlobalSecondaryIndexes": [{
    "Backfilling": boolean,
    "IndexArn": "string",
    "IndexName": "string",
    "IndexSizeBytes": number,
    "IndexStatus": "string",
    "ItemCount": number,
    "KeySchema": [{
      "AttributeName": "string",
      "KeyType": "string"
    }],
    "Projection": {
      "NonKeyAttributes": ["string"],
      "ProjectionType": "string"
    },
    "ProvisionedThroughput": {
      "LastDecreaseDateTime": "string",
      "LastIncreaseDateTime": "string",
      "NumberOfDecreasesToday": number,
      "ReadCapacityUnits": number,
      "WriteCapacityUnits": number
    }
  }],
  "GlobalTableVersion": "string",
  "ItemCount": number,
  "KeySchema": [{
    "AttributeName": "string",
    "KeyType": "string"
  }],
}
```

```
"LatestStreamArn": "string",
"LatestStreamLabel": "string",
"LocalSecondaryIndexes": [{
  "IndexArn": "string",
  "IndexName": "string",
  "KeySchema": [{
    "AttributeName": "string",
    "KeyType": "string"
  }],
  "Projection": {
    "NonKeyAttributes": ["string"],
    "ProjectionType": "string"
  }
}],
"ProvisionedThroughput": {
  "LastDecreaseDateTime": "string",
  "LastIncreaseDateTime": "string",
  "NumberOfDecreasesToday": number,
  "ReadCapacityUnits": number,
  "WriteCapacityUnits": number
},
"Replicas": [{
  "GlobalSecondaryIndexes": [{
    "IndexName": "string",
    "ProvisionedThroughputOverride": {
      "ReadCapacityUnits": number
    }
  }],
  "KmsMasterKeyId": "string",
  "ProvisionedThroughputOverride": {
    "ReadCapacityUnits": number
  },
  "RegionName": "string",
  "ReplicaStatus": "string",
  "ReplicaStatusDescription": "string"
}],
"RestoreSummary": {
  "RestoreDateTime": "string",
  "RestoreInProgress": boolean,
  "SourceBackupArn": "string",
  "SourceTableArn": "string"
},
"SseDescription": {
  "InaccessibleEncryptionDateTime": "string",
```

```
    "KmsMasterKeyArn": "string",
    "SseType": "string",
    "Status": "string"
  },
  "StreamSpecification": {
    "StreamEnabled": boolean,
    "StreamViewType": "string"
  },
  "TableId": "string",
  "TableName": "string",
  "TableSizeBytes": number,
  "TableStatus": "string"
},
"AwsEc2ClientVpnEndpoint": {
  "AuthenticationOptions": [
    {
      "MutualAuthentication": {
        "ClientRootCertificateChainArn": "string"
      },
      "Type": "string"
    }
  ],
  "ClientCidrBlock": "string",
  "ClientConnectOptions": {
    "Enabled": boolean
  },
  "ClientLoginBannerOptions": {
    "Enabled": boolean
  },
  "ClientVpnEndpointId": "string",
  "ConnectionLogOptions": {
    "Enabled": boolean
  },
  "Description": "string",
  "DnsServer": ["string"],
  "ServerCertificateArn": "string",
  "SecurityGroupIdSet": [
    "string"
  ],
  "SelfServicePortalUrl": "string",
  "SessionTimeoutHours": "integer",
  "SplitTunnel": boolean,
  "TransportProtocol": "string",
  "VpcId": "string",
```

```

    "VpnPort": integer
  },
  "AwsEc2Eip": {
    "AllocationId": "string",
    "AssociationId": "string",
    "Domain": "string",
    "InstanceId": "string",
    "NetworkBorderGroup": "string",
    "NetworkInterfaceId": "string",
    "NetworkInterfaceOwnerId": "string",
    "PrivateIpAddress": "string",
    "PublicIp": "string",
    "PublicIpv4Pool": "string"
  },
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "string",
    "ImageId": "string",
    "IPv4Addresses": ["string"],
    "IPv6Addresses": ["string"],
    "KeyName": "string",
    "LaunchedAt": "string",
    "MetadataOptions": {
      "HttpEndpoint": "string",
      "HttpProtocolIpv6": "string",
      "HttpPutResponseHopLimit": number,
      "HttpTokens": "string",
      "InstanceMetadataTags": "string"
    },
    "Monitoring": {
      "State": "string"
    },
    "NetworkInterfaces": [{
      "NetworkInterfaceId": "string"
    }],
    "SubnetId": "string",
    "Type": "string",
    "VirtualizationType": "string",
    "VpcId": "string"
  },
  "AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "string",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "string",

```

```

"ImageId": "string",
"LatestVersionNumber": "string",
"LaunchTemplateData": {
  "BlockDeviceMappings": [{
    "DeviceName": "string",
    "Ebs": {
      "DeleteonTermination": boolean,
      "Encrypted": boolean,
      "SnapshotId": "string",
      "VolumeSize": number,
      "VolumeType": "string"
    }
  }],
  "MetadataOptions": {
    "HttpTokens": "string",
    "HttpPutResponseHopLimit" : number
  },
  "Monitoring": {
    "Enabled": boolean
  },
  "NetworkInterfaces": [{
    "AssociatePublicIpAddress" : boolean
  }]
},
"LaunchTemplateName": "string",
"LicenseSpecifications": ["string"],
"SecurityGroupIds": ["string"],
"SecurityGroups": ["string"],
"TagSpecifications": ["string"]
},
"AwsEc2NetworkAcl": {
  "Associations": [{
    "NetworkAclAssociationId": "string",
    "NetworkAclId": "string",
    "SubnetId": "string"
  }],
  "Entries": [{
    "CidrBlock": "string",
    "Egress": boolean,
    "IcmpTypeCode": {
      "Code": number,
      "Type": number
    },
    "Ipv6CidrBlock": "string",

```



```

    "PortRange": {
      "From": number,
      "To": number
    },
    "Protocol": "string",
    "RuleAction": "string",
    "RuleNumber": number
  ]],
  "IsDefault": boolean,
  "NetworkAclId": "string",
  "OwnerId": "string",
  "VpcId": "string"
},
"AwsEc2NetworkInterface": {
  "Attachment": {
    "AttachmentId": "string",
    "AttachTime": "string",
    "DeleteOnTermination": boolean,
    "DeviceIndex": number,
    "InstanceId": "string",
    "InstanceOwnerId": "string",
    "Status": "string"
  },
  "Ipv6Addresses": [{
    "Ipv6Address": "string"
  }],
  "NetworkInterfaceId": "string",
  "PrivateIpAddresses": [{
    "PrivateDnsName": "string",
    "PrivateIpAddress": "string"
  }],
  "PublicDnsName": "string",
  "PublicIp": "string",
  "SecurityGroups": [{
    "GroupId": "string",
    "GroupName": "string"
  }],
  "SourceDestCheck": boolean
},
"AwsEc2RouteTable": {
  "AssociationSet": [{
    "AssociationState": {
      "State": "string"
    }
  }],

```

```

    "Main": boolean,
    "RouteTableAssociationId": "string",
    "RouteTableId": "string"
  ]],
  "PropagatingVgwSet": [],
  "RouteTableId": "string",
  "RouteSet": [
    {
      "DestinationCidrBlock": "string",
      "GatewayId": "string",
      "Origin": "string",
      "State": "string"
    },
    {
      "DestinationCidrBlock": "string",
      "GatewayId": "string",
      "Origin": "string",
      "State": "string"
    }
  ],
  "VpcId": "string"
},
"AwsEc2SecurityGroup": {
  "GroupId": "string",
  "GroupName": "string",
  "IpPermissions": [{
    "FromPort": number,
    "IpProtocol": "string",
    "IpRanges": [{
      "CidrIp": "string"
    }],
    "Ipv6Ranges": [{
      "CidrIpv6": "string"
    }],
    "PrefixListIds": [{
      "PrefixListId": "string"
    }],
    "ToPort": number,
    "UserIdGroupPairs": [{
      "GroupId": "string",
      "GroupName": "string",
      "PeeringStatus": "string",
      "UserId": "string",
      "VpcId": "string",

```

```

    "VpcPeeringConnectionId": "string"
  ]
}],
"IpPermissionsEgress": [{
  "FromPort": number,
  "IpProtocol": "string",
  "IpRanges": [{
    "CidrIp": "string"
  }],
  "Ipv6Ranges": [{
    "CidrIpv6": "string"
  }],
  "PrefixListIds": [{
    "PrefixListId": "string"
  }],
  "ToPort": number,
  "UserIdGroupPairs": [{
    "GroupId": "string",
    "GroupName": "string",
    "PeeringStatus": "string",
    "UserId": "string",
    "VpcId": "string",
    "VpcPeeringConnectionId": "string"
  }]
}],
"OwnerId": "string",
"VpcId": "string"
},
"AwsEc2Subnet": {
  "AssignIpv6AddressOnCreation": boolean,
  "AvailabilityZone": "string",
  "AvailabilityZoneId": "string",
  "AvailableIpAddressCount": number,
  "CidrBlock": "string",
  "DefaultForAz": boolean,
  "Ipv6CidrBlockAssociationSet": [{
    "AssociationId": "string",
    "Ipv6CidrBlock": "string",
    "CidrBlockState": "string"
  }],
  "MapPublicIpOnLaunch": boolean,
  "OwnerId": "string",
  "State": "string",
  "SubnetArn": "string",

```

```
"SubnetId": "string",
"VpcId": "string"
},
"AwsEc2TransitGateway": {
  "AmazonSideAsn": number,
  "AssociationDefaultRouteTableId": "string",
  "AutoAcceptSharedAttachments": "string",
  "DefaultRouteTableAssociation": "string",
  "DefaultRouteTablePropagation": "string",
  "Description": "string",
  "DnsSupport": "string",
  "Id": "string",
  "MulticastSupport": "string",
  "PropagationDefaultRouteTableId": "string",
  "TransitGatewayCidrBlocks": ["string"],
  "VpnEcmpSupport": "string"
},
"AwsEc2Volume": {
  "Attachments": [{
    "AttachTime": "string",
    "DeleteOnTermination": boolean,
    "InstanceId": "string",
    "Status": "string"
  }],
  "CreateTime": "string",
  "DeviceName": "string",
  "Encrypted": boolean,
  "KmsKeyId": "string",
  "Size": number,
  "SnapshotId": "string",
  "Status": "string",
  "VolumeId": "string",
  "VolumeScanStatus": "string",
  "VolumeType": "string"
},
"AwsEc2Vpc": {
  "CidrBlockAssociationSet": [{
    "AssociationId": "string",
    "CidrBlock": "string",
    "CidrBlockState": "string"
  }],
  "DhcpOptionsId": "string",
  "Ipv6CidrBlockAssociationSet": [{
    "AssociationId": "string",
```

```

    "CidrBlockState": "string",
    "Ipv6CidrBlock": "string"
  ]],
  "State": "string"
},
"AwsEc2VpcEndpointService": {
  "AcceptanceRequired": boolean,
  "AvailabilityZones": ["string"],
  "BaseEndpointDnsNames": ["string"],
  "ManagesVpcEndpoints": boolean,
  "GatewayLoadBalancerArns": ["string"],
  "NetworkLoadBalancerArns": ["string"],
  "PrivateDnsName": "string",
  "ServiceId": "string",
  "ServiceName": "string",
  "ServiceState": "string",
  "ServiceType": [{
    "ServiceType": "string"
  }]
},
"AwsEc2VpcPeeringConnection": {
  "AcceptorVpcInfo": {
    "CidrBlock": "string",
    "CidrBlockSet": [{
      "CidrBlock": "string"
    }],
    "Ipv6CidrBlockSet": [{
      "Ipv6CidrBlock": "string"
    }],
    "OwnerId": "string",
    "PeeringOptions": {
      "AllowDnsResolutionFromRemoteVpc": boolean,
      "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
      "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
    },
    "Region": "string",
    "VpcId": "string"
  },
  "ExpirationTime": "string",
  "RequesterVpcInfo": {
    "CidrBlock": "string",
    "CidrBlockSet": [{
      "CidrBlock": "string"
    }],

```

```

    "Ipv6CidrBlockSet": [{
      "Ipv6CidrBlock": "string"
    }],
    "OwnerId": "string",
    "PeeringOptions": {
      "AllowDnsResolutionFromRemoteVpc": boolean,
      "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
      "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
    },
    "Region": "string",
    "VpcId": "string"
  },
  "Status": {
    "Code": "string",
    "Message": "string"
  },
  "VpcPeeringConnectionId": "string"
},
"AwsEcrContainerImage": {
  "Architecture": "string",
  "ImageDigest": "string",
  "ImagePublishedAt": "string",
  "ImageTags": ["string"],
  "RegistryId": "string",
  "RepositoryName": "string"
},
"AwsEcrRepository": {
  "Arn": "string",
  "ImageScanningConfiguration": {
    "ScanOnPush": boolean
  },
  "ImageTagMutability": "string",
  "LifecyclePolicy": {
    "LifecyclePolicyText": "string",
    "RegistryId": "string"
  },
  "RepositoryName": "string",
  "RepositoryPolicyText": "string"
},
"AwsEcsCluster": {
  "ActiveServicesCount": number,
  "CapacityProviders": ["string"],
  "ClusterArn": "string",
  "ClusterName": "string",

```

```

"ClusterSettings": [{
  "Name": "string",
  "Value": "string"
}],
"Configuration": {
  "ExecuteCommandConfiguration": {
    "KmsKeyId": "string",
    "LogConfiguration": {
      "CloudWatchEncryptionEnabled": boolean,
      "CloudWatchLogGroupName": "string",
      "S3BucketName": "string",
      "S3EncryptionEnabled": boolean,
      "S3KeyPrefix": "string"
    },
    "Logging": "string"
  },
  "DefaultCapacityProviderStrategy": [{
    "Base": number,
    "CapacityProvider": "string",
    "Weight": number
  }],
  "RegisteredContainerInstancesCount": number,
  "RunningTasksCount": number,
  "Status": "string"
},
"AwsEcsContainer": {
  "Image": "string",
  "MountPoints": [{
    "ContainerPath": "string",
    "SourceVolume": "string"
  }],
  "Name": "string",
  "Privileged": boolean
},
"AwsEcsService": {
  "CapacityProviderStrategy": [{
    "Base": number,
    "CapacityProvider": "string",
    "Weight": number
  }],
  "Cluster": "string",
  "DeploymentConfiguration": {
    "DeploymentCircuitBreaker": {

```

```
    "Enable": boolean,
    "Rollback": boolean
  },
  "MaximumPercent": number,
  "MinimumHealthyPercent": number
},
"DeploymentController": {
  "Type": "string"
},
"DesiredCount": number,
"EnableEcsManagedTags": boolean,
"EnableExecuteCommand": boolean,
"HealthCheckGracePeriodSeconds": number,
"LaunchType": "string",
"LoadBalancers": [{
  "ContainerName": "string",
  "ContainerPort": number,
  "LoadBalancerName": "string",
  "TargetGroupArn": "string"
}],
"Name": "string",
"NetworkConfiguration": {
  "AwsVpcConfiguration": {
    "AssignPublicIp": "string",
    "SecurityGroups": ["string"],
    "Subnets": ["string"]
  }
},
"PlacementConstraints": [{
  "Expression": "string",
  "Type": "string"
}],
"PlacementStrategies": [{
  "Field": "string",
  "Type": "string"
}],
"PlatformVersion": "string",
"PropagateTags": "string",
"Role": "string",
"SchedulingStrategy": "string",
"ServiceArn": "string",
"ServiceName": "string",
"ServiceRegistries": [{
  "ContainerName": "string",
```



```

    "ContainerPort": number,
    "Port": number,
    "RegistryArn": "string"
  ]],
  "TaskDefinition": "string"
},
"AwsEcsTask": {
  "CreatedAt": "string",
  "ClusterArn": "string",
  "Group": "string",
  "StartedAt": "string",
  "StartedBy": "string",
  "TaskDefinitionArn": "string",
  "Version": number,
  "Volumes": [{
    "Name": "string",
    "Host": {
      "SourcePath": "string"
    }
  }],
  "Containers": [{
    "Image": "string",
    "MountPoints": [{
      "ContainerPath": "string",
      "SourceVolume": "string"
    }],
    "Name": "string",
    "Privileged": boolean
  }]
},
"AwsEcsTaskDefinition": {
  "ContainerDefinitions": [{
    "Command": ["string"],
    "Cpu": number,
    "DependsOn": [{
      "Condition": "string",
      "ContainerName": "string"
    }],
    "DisableNetworking": boolean,
    "DnsSearchDomains": ["string"],
    "DnsServers": ["string"],
    "DockerLabels": {
      "string": "string"
    }
  }],

```

```
"DockerSecurityOptions": ["string"],
"EntryPoint": ["string"],
"Environment": [{
  "Name": "string",
  "Value": "string"
}],
"EnvironmentFiles": [{
  "Type": "string",
  "Value": "string"
}],
"Essential": boolean,
"ExtraHosts": [{
  "Hostname": "string",
  "IpAddress": "string"
}],
"FirelensConfiguration": {
  "Options": {
    "string": "string"
  },
  "Type": "string"
},
"HealthCheck": {
  "Command": ["string"],
  "Interval": number,
  "Retries": number,
  "StartPeriod": number,
  "Timeout": number
},
"Hostname": "string",
"Image": "string",
"Interactive": boolean,
"Links": ["string"],
"LinuxParameters": {
  "Capabilities": {
    "Add": ["string"],
    "Drop": ["string"]
  },
  "Devices": [{
    "ContainerPath": "string",
    "HostPath": "string",
    "Permissions": ["string"]
  }],
  "InitProcessEnabled": boolean,
  "MaxSwap": number,
```

```
"SharedMemorySize": number,
"Swappiness": number,
"Tmpfs": [{
  "ContainerPath": "string",
  "MountOptions": ["string"],
  "Size": number
}]
},
"LogConfiguration": {
  "LogDriver": "string",
  "Options": {
    "string": "string"
  },
  "SecretOptions": [{
    "Name": "string",
    "ValueFrom": "string"
  }]
},
"Memory": number,
"MemoryReservation": number,
"MountPoints": [{
  "ContainerPath": "string",
  "ReadOnly": boolean,
  "SourceVolume": "string"
}],
"Name": "string",
"PortMappings": [{
  "ContainerPort": number,
  "HostPort": number,
  "Protocol": "string"
}],
"Privileged": boolean,
"PseudoTerminal": boolean,
"ReadonlyRootFilesystem": boolean,
"RepositoryCredentials": {
  "CredentialsParameter": "string"
},
"ResourceRequirements": [{
  "Type": "string",
  "Value": "string"
}],
"Secrets": [{
  "Name": "string",
  "ValueFrom": "string"
}]
```

```
    }],  
    "StartTimeout": number,  
    "StopTimeout": number,  
    "SystemControls": [{  
      "Namespace": "string",  
      "Value": "string"  
    }],  
    "Ulimits": [{  
      "HardLimit": number,  
      "Name": "string",  
      "SoftLimit": number  
    }],  
    "User": "string",  
    "VolumesFrom": [{  
      "ReadOnly": boolean,  
      "SourceContainer": "string"  
    }],  
    "WorkingDirectory": "string"  
  }],  
  "Cpu": "string",  
  "ExecutionRoleArn": "string",  
  "Family": "string",  
  "InferenceAccelerators": [{  
    "DeviceName": "string",  
    "DeviceType": "string"  
  }],  
  "IpcMode": "string",  
  "Memory": "string",  
  "NetworkMode": "string",  
  "PidMode": "string",  
  "PlacementConstraints": [{  
    "Expression": "string",  
    "Type": "string"  
  }],  
  "ProxyConfiguration": {  
    "ContainerName": "string",  
    "ProxyConfigurationProperties": [{  
      "Name": "string",  
      "Value": "string"  
    }],  
    "Type": "string"  
  },  
  "RequiresCompatibilities": ["string"],  
  "Status": "string",
```

```

"TaskRoleArn": "string",
"Volumes": [{
  "DockerVolumeConfiguration": {
    "Autoprovision": boolean,
    "Driver": "string",
    "DriverOpts": {
      "string": "string"
    },
    "Labels": {
      "string": "string"
    },
    "Scope": "string"
  },
  "EfsVolumeConfiguration": {
    "AuthorizationConfig": {
      "AccessPointId": "string",
      "Iam": "string"
    },
    "FilesystemId": "string",
    "RootDirectory": "string",
    "TransitEncryption": "string",
    "TransitEncryptionPort": number
  },
  "Host": {
    "SourcePath": "string"
  },
  "Name": "string"
}]
},
"AwsEfsAccessPoint": {
  "AccessPointId": "string",
  "Arn": "string",
  "ClientToken": "string",
  "FileSystemId": "string",
  "PosixUser": {
    "Gid": "string",
    "SecondaryGids": ["string"],
    "Uid": "string"
  },
  "RootDirectory": {
    "CreationInfo": {
      "OwnerGid": "string",
      "OwnerUid": "string",
      "Permissions": "string"
    }
  }
}

```

```

    },
    "Path": "string"
  }
},
"AwsEksCluster": {
  "Arn": "string",
  "CertificateAuthorityData": "string",
  "ClusterStatus": "string",
  "Endpoint": "string",
  "Logging": {
    "ClusterLogging": [{
      "Enabled": boolean,
      "Types": ["string"]
    }]
  },
  "Name": "string",
  "ResourcesVpcConfig": {
    "EndpointPublicAccess": boolean,
    "SecurityGroupIds": ["string"],
    "SubnetIds": ["string"]
  },
  "RoleArn": "string",
  "Version": "string"
},
"AwsElasticBeanstalkEnvironment": {
  "ApplicationName": "string",
  "Cname": "string",
  "DateCreated": "string",
  "DateUpdated": "string",
  "Description": "string",
  "EndpointUrl": "string",
  "EnvironmentArn": "string",
  "EnvironmentId": "string",
  "EnvironmentLinks": [{
    "EnvironmentName": "string",
    "LinkName": "string"
  }],
  "EnvironmentName": "string",
  "OptionSettings": [{
    "Namespace": "string",
    "OptionName": "string",
    "ResourceName": "string",
    "Value": "string"
  }],

```

```
"PlatformArn": "string",
"SolutionStackName": "string",
"Status": "string",
"Tier": {
  "Name": "string",
  "Type": "string",
  "Version": "string"
},
"VersionLabel": "string"
},
"AwsElasticSearchDomain": {
  "AccessPolicies": "string",
  "DomainStatus": {
    "DomainId": "string",
    "DomainName": "string",
    "Endpoint": "string",
    "Endpoints": {
      "string": "string"
    }
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": boolean,
    "TLSSecurityPolicy": "string"
  },
  "ElasticsearchClusterConfig": {
    "DedicatedMasterCount": number,
    "DedicatedMasterEnabled": boolean,
    "DedicatedMasterType": "string",
    "InstanceCount": number,
    "InstanceType": "string",
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": number
    },
    "ZoneAwarenessEnabled": boolean
  },
  "ElasticsearchVersion": "string",
  "EncryptionAtRestOptions": {
    "Enabled": boolean,
    "KmsKeyId": "string"
  },
  "LogPublishingOptions": {
    "AuditLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    }
  }
}
```

```

    },
    "IndexSlowLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    },
    "SearchSlowLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    }
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": boolean
  },
  "ServiceSoftwareOptions": {
    "AutomatedUpdateDate": "string",
    "Cancellable": boolean,
    "CurrentVersion": "string",
    "Description": "string",
    "NewVersion": "string",
    "UpdateAvailable": boolean,
    "UpdateStatus": "string"
  },
  "VPCOptions": {
    "AvailabilityZones": [
      "string"
    ],
    "SecurityGroupIds": [
      "string"
    ],
    "SubnetIds": [
      "string"
    ],
    "VPCId": "string"
  }
},
"AwsElbLoadBalancer": {
  "AvailabilityZones": ["string"],
  "BackendServerDescriptions": [{
    "InstancePort": number,
    "PolicyNames": ["string"]
  }],
  "CanonicalHostedZoneName": "string",
  "CanonicalHostedZoneNameID": "string",
  "CreatedTime": "string",

```



```
"DnsName": "string",
"HealthCheck": {
  "HealthyThreshold": number,
  "Interval": number,
  "Target": "string",
  "Timeout": number,
  "UnhealthyThreshold": number
},
"Instances": [{
  "InstanceId": "string"
}],
"ListenerDescriptions": [{
  "Listener": {
    "InstancePort": number,
    "InstanceProtocol": "string",
    "LoadBalancerPort": number,
    "Protocol": "string",
    "SslCertificateId": "string"
  },
  "PolicyNames": ["string"]
}],
"LoadBalancerAttributes": {
  "AccessLog": {
    "EmitInterval": number,
    "Enabled": boolean,
    "S3BucketName": "string",
    "S3BucketPrefix": "string"
  },
  "ConnectionDraining": {
    "Enabled": boolean,
    "Timeout": number
  },
  "ConnectionSettings": {
    "IdleTimeout": number
  },
  "CrossZoneLoadBalancing": {
    "Enabled": boolean
  },
  "AdditionalAttributes": [{
    "Key": "string",
    "Value": "string"
  }]
},
"LoadBalancerName": "string",
```

```

"Policies": {
  "AppCookieStickinessPolicies": [{
    "CookieName": "string",
    "PolicyName": "string"
  }],
  "LbCookieStickinessPolicies": [{
    "CookieExpirationPeriod": number,
    "PolicyName": "string"
  }],
  "OtherPolicies": ["string"]
},
"Scheme": "string",
"SecurityGroups": ["string"],
"SourceSecurityGroup": {
  "GroupName": "string",
  "OwnerAlias": "string"
},
"Subnets": ["string"],
"VpcId": "string"
},
"AwsElbv2LoadBalancer": {
  "AvailabilityZones": {
    "SubnetId": "string",
    "ZoneName": "string"
  },
  "CanonicalHostedZoneId": "string",
  "CreatedTime": "string",
  "DNSName": "string",
  "IpAddressType": "string",
  "LoadBalancerAttributes": [{
    "Key": "string",
    "Value": "string"
  }],
  "Scheme": "string",
  "SecurityGroups": ["string"],
  "State": {
    "Code": "string",
    "Reason": "string"
  },
  "Type": "string",
  "VpcId": "string"
},
"AwsEventSchemasRegistry": {
  "Description": "string",

```

```

    "RegistryArn": "string",
    "RegistryName": "string"
  },
  "AwsEventsEndpoint": {
    "Arn": "string",
    "Description": "string",
    "EndpointId": "string",
    "EndpointUrl": "string",
    "EventBuses": [
      {
        "EventBusArn": "string"
      },
      {
        "EventBusArn": "string"
      }
    ],
    "Name": "string",
    "ReplicationConfig": {
      "State": "string"
    },
    "RoleArn": "string",
    "RoutingConfig": {
      "FailoverConfig": {
        "Primary": {
          "HealthCheck": "string"
        },
        "Secondary": {
          "Route": "string"
        }
      }
    },
    "State": "string"
  },
  "AwsEventsEventBus": {
    "Arn": "string",
    "Name": "string",
    "Policy": "string"
  },
  "AwsGuardDutyDetector": {
    "FindingPublishingFrequency": "string",
    "ServiceRole": "string",
    "Status": "string",
    "DataSources": {
      "CloudTrail": {

```

```
    "Status": "string"
  },
  "DnsLogs": {
    "Status": "string"
  },
  "FlowLogs": {
    "Status": "string"
  },
  "S3Logs": {
    "Status": "string"
  },
  "Kubernetes": {
    "AuditLogs": {
      "Status": "string"
    }
  },
  "MalwareProtection": {
    "ScanEc2InstanceWithFindings": {
      "EbsVolumes": {
        "Status": "string"
      }
    },
    "ServiceRole": "string"
  }
},
"AwsIamAccessKey": {
  "AccessKeyId": "string",
  "AccountId": "string",
  "CreatedAt": "string",
  "PrincipalId": "string",
  "PrincipalName": "string",
  "PrincipalType": "string",
  "SessionContext": {
    "Attributes": {
      "CreationDate": "string",
      "MfaAuthenticated": boolean
    }
  },
  "SessionIssuer": {
    "AccountId": "string",
    "Arn": "string",
    "PrincipalId": "string",
    "Type": "string",
    "UserName": "string"
  }
}
```

```
    }
  },
  "Status": "string"
},
"AwsIamGroup": {
  "AttachedManagedPolicies": [{
    "PolicyArn": "string",
    "PolicyName": "string"
  }],
  "CreateDate": "string",
  "GroupId": "string",
  "GroupName": "string",
  "GroupPolicyList": [{
    "PolicyName": "string"
  }],
  "Path": "string"
},
"AwsIamPolicy": {
  "AttachmentCount": number,
  "CreateDate": "string",
  "DefaultVersionId": "string",
  "Description": "string",
  "IsAttachable": boolean,
  "Path": "string",
  "PermissionsBoundaryUsageCount": number,
  "PolicyId": "string",
  "PolicyName": "string",
  "PolicyVersionList": [{
    "CreateDate": "string",
    "IsDefaultVersion": boolean,
    "VersionId": "string"
  }],
  "UpdateDate": "string"
},
"AwsIamRole": {
  "AssumeRolePolicyDocument": "string",
  "AttachedManagedPolicies": [{
    "PolicyArn": "string",
    "PolicyName": "string"
  }],
  "CreateDate": "string",
  "InstanceProfileList": [{
    "Arn": "string",
    "CreateDate": "string",
```

```

    "InstanceProfileId": "string",
    "InstanceProfileName": "string",
    "Path": "string",
    "Roles": [{
      "Arn": "string",
      "AssumeRolePolicyDocument": "string",
      "CreateDate": "string",
      "Path": "string",
      "RoleId": "string",
      "RoleName": "string"
    }]
  }],
  "MaxSessionDuration": number,
  "Path": "string",
  "PermissionsBoundary": {
    "PermissionsBoundaryArn": "string",
    "PermissionsBoundaryType": "string"
  },
  "RoleId": "string",
  "RoleName": "string",
  "RolePolicyList": [{
    "PolicyName": "string"
  }]
},
"AwsIamUser": {
  "AttachedManagedPolicies": [{
    "PolicyArn": "string",
    "PolicyName": "string"
  }],
  "CreateDate": "string",
  "GroupList": ["string"],
  "Path": "string",
  "PermissionsBoundary": {
    "PermissionsBoundaryArn": "string",
    "PermissionsBoundaryType": "string"
  },
  "UserId": "string",
  "UserName": "string",
  "UserPolicyList": [{
    "PolicyName": "string"
  }]
},
"AwsKinesisStream": {
  "Arn": "string",

```

```
"Name": "string",
"RetentionPeriodHours": number,
"ShardCount": number,
"StreamEncryption": {
  "EncryptionType": "string",
  "KeyId": "string"
}
},
"AwsKmsKey": {
  "AWSAccountId": "string",
  "CreationDate": "string",
  "Description": "string",
  "KeyId": "string",
  "KeyManager": "string",
  "KeyRotationStatus": boolean,
  "KeyState": "string",
  "Origin": "string"
},
"AwsLambdaFunction": {
  "Architectures": [
    "string"
  ],
  "Code": {
    "S3Bucket": "string",
    "S3Key": "string",
    "S3ObjectVersion": "string",
    "ZipFile": "string"
  },
  "CodeSha256": "string",
  "DeadLetterConfig": {
    "TargetArn": "string"
  },
  "Environment": {
    "Variables": {
      "Stage": "string"
    }
  },
  "Error": {
    "ErrorCode": "string",
    "Message": "string"
  }
},
"FunctionName": "string",
"Handler": "string",
"KmsKeyArn": "string",
```

```
"LastModified": "string",
"Layers": {
  "Arn": "string",
  "CodeSize": number
},
"PackageType": "string",
"RevisionId": "string",
"Role": "string",
"Runtime": "string",
"Timeout": integer,
"TracingConfig": {
  "Mode": "string"
},
"Version": "string",
"VpcConfig": {
  "SecurityGroupIds": ["string"],
  "SubnetIds": ["string"]
},
"MasterArn": "string",
"MemorySize": number
},
"AwsLambdaLayerVersion": {
  "CompatibleRuntimes": [
    "string"
  ],
  "CreateDate": "string",
  "Version": number
},
"AwsMskCluster": {
  "ClusterInfo": {
    "ClientAuthentication": {
      "Sasl": {
        "Scram": {
          "Enabled": boolean
        },
        "Iam": {
          "Enabled": boolean
        }
      },
      "Tls": {
        "CertificateAuthorityArnList": [],
        "Enabled": boolean
      },
      "Unauthenticated": {
```



```

    "Enabled": boolean
  },
  "ClusterName": "string",
  "CurrentVersion": "string",
  "EncryptionInfo": {
    "EncryptionAtRest": {
      "DataVolumeKMSKeyId": "string"
    },
    "EncryptionInTransit": {
      "ClientBroker": "string",
      "InCluster": boolean
    }
  },
  "EnhancedMonitoring": "string",
  "NumberOfBrokerNodes": integer
},
"AwsNetworkFirewallFirewall": {
  "DeleteProtection": boolean,
  "Description": "string",
  "FirewallArn": "string",
  "FirewallId": "string",
  "FirewallName": "string",
  "FirewallPolicyArn": "string",
  "FirewallPolicyChangeProtection": boolean,
  "SubnetChangeProtection": boolean,
  "SubnetMappings": [{
    "SubnetId": "string"
  }],
  "VpcId": "string"
},
"AwsNetworkFirewallFirewallPolicy": {
  "Description": "string",
  "FirewallPolicy": {
    "StatefulRuleGroupReferences": [{
      "ResourceArn": "string"
    }],
    "StatelessCustomActions": [{
      "ActionDefinition": {
        "PublishMetricAction": {
          "Dimensions": [{
            "Value": "string"
          }
        ]
      }
    }
  ]
}

```

```

    }
  },
  "ActionName": "string"
}],
"StatelessDefaultActions": ["string"],
"StatelessFragmentDefaultActions": ["string"],
"StatelessRuleGroupReferences": [{
  "Priority": number,
  "ResourceArn": "string"
}]
},
"FirewallPolicyArn": "string",
"FirewallPolicyId": "string",
"FirewallPolicyName": "string"
},
"AwsNetworkFirewallRuleGroup": {
  "Capacity": number,
  "Description": "string",
  "RuleGroup": {
    "RulesSource": {
      "RulesSourceList": {
        "GeneratedRulesType": "string",
        "Targets": ["string"],
        "TargetTypes": ["string"]
      },
      "RulesString": "string",
      "StatefulRules": [{
        "Action": "string",
        "Header": {
          "Destination": "string",
          "DestinationPort": "string",
          "Direction": "string",
          "Protocol": "string",
          "Source": "string",
          "SourcePort": "string"
        },
        "RuleOptions": [{
          "Keyword": "string",
          "Settings": ["string"]
        }]
      }],
      "StatelessRulesAndCustomActions": {
        "CustomActions": [{
          "ActionDefinition": {

```

```

    "PublishMetricAction": {
      "Dimensions": [{
        "Value": "string"
      }]
    },
    "ActionName": "string"
  ]],
  "StatelessRules": [{
    "Priority": number,
    "RuleDefinition": {
      "Actions": ["string"],
      "MatchAttributes": {
        "DestinationPorts": [{
          "FromPort": number,
          "ToPort": number
        }],
        "Destinations": [{
          "AddressDefinition": "string"
        }],
        "Protocols": [number],
        "SourcePorts": [{
          "FromPort": number,
          "ToPort": number
        }],
        "Sources": [{
          "AddressDefinition": "string"
        }],
        "TcpFlags": [{
          "Flags": ["string"],
          "Masks": ["string"]
        }]
      }
    }
  ]],
  "RuleVariables": {
    "IpSets": {
      "Definition": ["string"]
    },
    "PortSets": {
      "Definition": ["string"]
    }
  }
}

```

```

    }
  },
  "RuleGroupArn": "string",
  "RuleGroupId": "string",
  "RuleGroupName": "string",
  "Type": "string"
},
"AwsOpenSearchServiceDomain": {
  "AccessPolicies": "string",
  "AdvancedSecurityOptions": {
    "Enabled": boolean,
    "InternalUserDatabaseEnabled": boolean,
    "MasterUserOptions": {
      "MasterUserArn": "string",
      "MasterUserName": "string",
      "MasterUserPassword": "string"
    }
  },
  "Arn": "string",
  "ClusterConfig": {
    "DedicatedMasterCount": number,
    "DedicatedMasterEnabled": boolean,
    "DedicatedMasterType": "string",
    "InstanceCount": number,
    "InstanceType": "string",
    "WarmCount": number,
    "WarmEnabled": boolean,
    "WarmType": "string",
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": number
    },
    "ZoneAwarenessEnabled": boolean
  },
  "DomainEndpoint": "string",
  "DomainEndpointOptions": {
    "CustomEndpoint": "string",
    "CustomEndpointCertificateArn": "string",
    "CustomEndpointEnabled": boolean,
    "EnforceHTTPS": boolean,
    "TLSSecurityPolicy": "string"
  },
  "DomainEndpoints": {
    "string": "string"
  }
},

```

```

"DomainName": "string",
"EncryptionAtRestOptions": {
  "Enabled": boolean,
  "KmsKeyId": "string"
},
"EngineVersion": "string",
"Id": "string",
"LogPublishingOptions": {
  "AuditLogs": {
    "CloudWatchLogsLogGroupArn": "string",
    "Enabled": boolean
  },
  "IndexSlowLogs": {
    "CloudWatchLogsLogGroupArn": "string",
    "Enabled": boolean
  },
  "SearchSlowLogs": {
    "CloudWatchLogsLogGroupArn": "string",
    "Enabled": boolean
  }
},
"NodeToNodeEncryptionOptions": {
  "Enabled": boolean
},
"ServiceSoftwareOptions": {
  "AutomatedUpdateDate": "string",
  "Cancellable": boolean,
  "CurrentVersion": "string",
  "Description": "string",
  "NewVersion": "string",
  "OptionalDeployment": boolean,
  "UpdateAvailable": boolean,
  "UpdateStatus": "string"
},
"VpcOptions": {
  "SecurityGroupIds": ["string"],
  "SubnetIds": ["string"]
},
"AwsRdsDbCluster": {
  "ActivityStreamStatus": "string",
  "AllocatedStorage": number,
  "AssociatedRoles": [{
    "RoleArn": "string",

```

```
"Status": "string"
}],
"AutoMinorVersionUpgrade": boolean,
"AvailabilityZones": ["string"],
"BackupRetentionPeriod": integer,
"ClusterCreateTime": "string",
"CopyTagsToSnapshot": boolean,
"CrossAccountClone": boolean,
"CustomEndpoints": ["string"],
"DatabaseName": "string",
"DbClusterIdentifier": "string",
"DbClusterMembers": [{
  "DbClusterParameterGroupStatus": "string",
  "DbInstanceIdentifier": "string",
  "IsClusterWriter": boolean,
  "PromotionTier": integer
}],
"DbClusterOptionGroupMemberships": [{
  "DbClusterOptionGroupName": "string",
  "Status": "string"
}],
"DbClusterParameterGroup": "string",
"DbClusterResourceId": "string",
"DbSubnetGroup": "string",
"DeletionProtection": boolean,
"DomainMemberships": [{
  "Domain": "string",
  "Fqdn": "string",
  "IamRoleName": "string",
  "Status": "string"
}],
"EnabledCloudwatchLogsExports": ["string"],
"Endpoint": "string",
"Engine": "string",
"EngineMode": "string",
"EngineVersion": "string",
"HostedZoneId": "string",
"HttpEndpointEnabled": boolean,
"IamDatabaseAuthenticationEnabled": boolean,
"KmsKeyId": "string",
"MasterUsername": "string",
"MultiAz": boolean,
"Port": integer,
"PreferredBackupWindow": "string",
```

```
"PreferredMaintenanceWindow": "string",
"ReaderEndpoint": "string",
"ReadReplicaIdentifiers": ["string"],
"Status": "string",
"StorageEncrypted": boolean,
"VpcSecurityGroups": [{
  "Status": "string",
  "VpcSecurityGroupId": "string"
}]
},
"AwsRdsDbClusterSnapshot": {
  "AllocatedStorage": integer,
  "AvailabilityZones": ["string"],
  "ClusterCreateTime": "string",
  "DbClusterIdentifier": "string",
  "DbClusterSnapshotAttributes": [{
    "AttributeName": "string",
    "AttributeValues": ["string"]
  }],
  "DbClusterSnapshotIdentifier": "string",
  "Engine": "string",
  "EngineVersion": "string",
  "IamDatabaseAuthenticationEnabled": boolean,
  "KmsKeyId": "string",
  "LicenseModel": "string",
  "MasterUsername": "string",
  "PercentProgress": integer,
  "Port": integer,
  "SnapshotCreateTime": "string",
  "SnapshotType": "string",
  "Status": "string",
  "StorageEncrypted": boolean,
  "VpcId": "string"
},
"AwsRdsDbInstance": {
  "AllocatedStorage": number,
  "AssociatedRoles": [{
    "RoleArn": "string",
    "FeatureName": "string",
    "Status": "string"
  }],
  "AutoMinorVersionUpgrade": boolean,
  "AvailabilityZone": "string",
  "BackupRetentionPeriod": number,
```

```
"CACertificateIdentifier": "string",
"CharacterSetName": "string",
"CopyTagsToSnapshot": boolean,
"DBClusterIdentifier": "string",
"DBInstanceClass": "string",
"DBInstanceIdentifier": "string",
"DbInstancePort": number,
"DbInstanceStatus": "string",
"DbiResourceId": "string",
"DBName": "string",
"DbParameterGroups": [{
  "DbParameterGroupName": "string",
  "ParameterApplyStatus": "string"
}],
"DbSecurityGroups": ["string"],
"DbSubnetGroup": {
  "DbSubnetGroupArn": "string",
  "DbSubnetGroupDescription": "string",
  "DbSubnetGroupName": "string",
  "SubnetGroupStatus": "string",
  "Subnets": [{
    "SubnetAvailabilityZone": {
      "Name": "string"
    },
    "SubnetIdentifier": "string",
    "SubnetStatus": "string"
  }],
  "VpcId": "string"
},
"DeletionProtection": boolean,
"Endpoint": {
  "Address": "string",
  "Port": number,
  "HostedZoneId": "string"
},
"DomainMemberships": [{
  "Domain": "string",
  "Fqdn": "string",
  "IamRoleName": "string",
  "Status": "string"
}],
"EnabledCloudwatchLogsExports": ["string"],
"Engine": "string",
"EngineVersion": "string",
```



```
"EnhancedMonitoringResourceArn": "string",
"IAMDatabaseAuthenticationEnabled": boolean,
"InstanceCreateTime": "string",
"Iops": number,
"KmsKeyId": "string",
"LatestRestorableTime": "string",
"LicenseModel": "string",
"ListenerEndpoint": {
  "Address": "string",
  "HostedZoneId": "string",
  "Port": number
},
"MasterUsername": "admin",
"MaxAllocatedStorage": number,
"MonitoringInterval": number,
"MonitoringRoleArn": "string",
"MultiAz": boolean,
"OptionGroupMemberships": [{
  "OptionGroupName": "string",
  "Status": "string"
}],
"PendingModifiedValues": {
  "AllocatedStorage": number,
  "BackupRetentionPeriod": number,
  "CaCertificateIdentifier": "string",
  "DbInstanceClass": "string",
  "DbInstanceIdentifier": "string",
  "DbSubnetGroupName": "string",
  "EngineVersion": "string",
  "Iops": number,
  "LicenseModel": "string",
  "MasterUserPassword": "string",
  "MultiAZ": boolean,
  "PendingCloudWatchLogsExports": {
    "LogTypesToDisable": ["string"],
    "LogTypesToEnable": ["string"]
  },
  "Port": number,
  "ProcessorFeatures": [{
    "Name": "string",
    "Value": "string"
  }],
  "StorageType": "string"
},
```

```

"PerformanceInsightsEnabled": boolean,
"PerformanceInsightsKmsKeyId": "string",
"PerformanceInsightsRetentionPeriod": number,
"PreferredBackupWindow": "string",
"PreferredMaintenanceWindow": "string",
"ProcessorFeatures": [{
  "Name": "string",
  "Value": "string"
}],
"PromotionTier": number,
"PubliclyAccessible": boolean,
"ReadReplicaDBClusterIdentifiers": ["string"],
"ReadReplicaDBInstanceIdentifiers": ["string"],
"ReadReplicaSourceDBInstanceIdentifier": "string",
"SecondaryAvailabilityZone": "string",
"StatusInfos": [{
  "Message": "string",
  "Normal": boolean,
  "Status": "string",
  "StatusType": "string"
}],
"StorageEncrypted": boolean,
"TdeCredentialArn": "string",
"Timezone": "string",
"VpcSecurityGroups": [{
  "VpcSecurityGroupId": "string",
  "Status": "string"
}]
},
"AwsRdsDbSecurityGroup": {
  "DbSecurityGroupArn": "string",
  "DbSecurityGroupDescription": "string",
  "DbSecurityGroupName": "string",
  "Ec2SecurityGroups": [{
    "Ec2SecurityGroupuId": "string",
    "Ec2SecurityGroupName": "string",
    "Ec2SecurityGroupOwnerId": "string",
    "Status": "string"
  }],
  "IpRanges": [{
    "CidrIp": "string",
    "Status": "string"
  }],
  "OwnerId": "string",

```

```

    "VpcId": "string"
  },
  "AwsRdsDbSnapshot": {
    "AllocatedStorage": integer,
    "AvailabilityZone": "string",
    "DbInstanceIdentifier": "string",
    "DbiResourceId": "string",
    "DbSnapshotIdentifier": "string",
    "Encrypted": boolean,
    "Engine": "string",
    "EngineVersion": "string",
    "IamDatabaseAuthenticationEnabled": boolean,
    "InstanceCreateTime": "string",
    "Iops": number,
    "KmsKeyId": "string",
    "LicenseModel": "string",
    "MasterUsername": "string",
    "OptionGroupName": "string",
    "PercentProgress": integer,
    "Port": integer,
    "ProcessorFeatures": [],
    "SnapshotCreateTime": "string",
    "SnapshotType": "string",
    "SourceDbSnapshotIdentifier": "string",
    "SourceRegion": "string",
    "Status": "string",
    "StorageType": "string",
    "TdeCredentialArn": "string",
    "Timezone": "string",
    "VpcId": "string"
  },
  "AwsRdsEventSubscription": {
    "CustomerAwsId": "string",
    "CustSubscriptionId": "string",
    "Enabled": boolean,
    "EventCategoriesList": ["string"],
    "EventSubscriptionArn": "string",
    "SnsTopicArn": "string",
    "SourceIdsList": ["string"],
    "SourceType": "string",
    "Status": "string",
    "SubscriptionCreationTime": "string"
  },
  "AwsRedshiftCluster": {

```

```
"AllowVersionUpgrade": boolean,
"AutomatedSnapshotRetentionPeriod": number,
"AvailabilityZone": "string",
"ClusterAvailabilityStatus": "string",
"ClusterCreateTime": "string",
"ClusterIdentifier": "string",
"ClusterNodes": [{
  "NodeRole": "string",
  "PrivateIPAddress": "string",
  "PublicIPAddress": "string"
}],
"ClusterParameterGroups": [{
  "ClusterParameterStatusList": [{
    "ParameterApplyErrorDescription": "string",
    "ParameterApplyStatus": "string",
    "ParameterName": "string"
  }],
  "ParameterApplyStatus": "string",
  "ParameterGroupName": "string"
}],
"ClusterPublicKey": "string",
"ClusterRevisionNumber": "string",
"ClusterSecurityGroups": [{
  "ClusterSecurityGroupName": "string",
  "Status": "string"
}],
"ClusterSnapshotCopyStatus": {
  "DestinationRegion": "string",
  "ManualSnapshotRetentionPeriod": number,
  "RetentionPeriod": number,
  "SnapshotCopyGrantName": "string"
},
"ClusterStatus": "string",
"ClusterSubnetGroupName": "string",
"ClusterVersion": "string",
"DBName": "string",
"DeferredMaintenanceWindows": [{
  "DeferMaintenanceEndTime": "string",
  "DeferMaintenanceIdentifier": "string",
  "DeferMaintenanceStartTime": "string"
}],
"ElasticIpStatus": {
  "ElasticIp": "string",
  "Status": "string"
}
```

```

},
"ElasticResizeNumberOfNodeOptions": "string",
"Encrypted": boolean,
"Endpoint": {
  "Address": "string",
  "Port": number
},
"EnhancedVpcRouting": boolean,
"ExpectedNextSnapshotScheduleTime": "string",
"ExpectedNextSnapshotScheduleTimeStatus": "string",
"HsmStatus": {
  "HsmClientCertificateIdentifier": "string",
  "HsmConfigurationIdentifier": "string",
  "Status": "string"
},
"IamRoles": [{
  "ApplyStatus": "string",
  "IamRoleArn": "string"
}],
"KmsKeyId": "string",
"LoggingStatus": {
  "BucketName": "string",
  "LastFailureMessage": "string",
  "LastFailureTime": "string",
  "LastSuccessfulDeliveryTime": "string",
  "LoggingEnabled": boolean,
  "S3KeyPrefix": "string"
},
"MaintenanceTrackName": "string",
"ManualSnapshotRetentionPeriod": number,
"MasterUsername": "string",
"NextMaintenanceWindowStartTime": "string",
"NodeType": "string",
"NumberOfNodes": number,
"PendingActions": ["string"],
"PendingModifiedValues": {
  "AutomatedSnapshotRetentionPeriod": number,
  "ClusterIdentifier": "string",
  "ClusterType": "string",
  "ClusterVersion": "string",
  "EncryptionType": "string",
  "EnhancedVpcRouting": boolean,
  "MaintenanceTrackName": "string",
  "MasterUserPassword": "string",

```

```

    "NodeType": "string",
    "NumberOfNodes": number,
    "PubliclyAccessible": "string"
  },
  "PreferredMaintenanceWindow": "string",
  "PubliclyAccessible": boolean,
  "ResizeInfo": {
    "AllowCancelResize": boolean,
    "ResizeType": "string"
  },
  "RestoreStatus": {
    "CurrentRestoreRateInMegaBytesPerSecond": number,
    "ElapsedTimeInSeconds": number,
    "EstimatedTimeToCompletionInSeconds": number,
    "ProgressInMegaBytes": number,
    "SnapshotSizeInMegaBytes": number,
    "Status": "string"
  },
  "SnapshotScheduleIdentifier": "string",
  "SnapshotScheduleState": "string",
  "VpcId": "string",
  "VpcSecurityGroups": [{
    "Status": "string",
    "VpcSecurityGroupId": "string"
  }]
},
"AwsRoute53HostedZone": {
  "HostedZone": {
    "Id": "string",
    "Name": "string",
    "Config": {
      "Comment": "string"
    }
  },
  "NameServers": ["string"],
  "QueryLoggingConfig": {
    "CloudWatchLogsLogGroupArn": {
      "CloudWatchLogsLogGroupArn": "string",
      "Id": "string",
      "HostedZoneId": "string"
    }
  },
  "Vpcs": [
    {

```

```

    "Id": "string",
    "Region": "string"
  }
],
},
"AwsS3AccessPoint": {
  "AccessPointArn": "string",
  "Alias": "string",
  "Bucket": "string",
  "BucketAccountId": "string",
  "Name": "string",
  "NetworkOrigin": "string",
  "PublicAccessBlockConfiguration": {
    "BlockPublicAcls": boolean,
    "BlockPublicPolicy": boolean,
    "IgnorePublicAcls": boolean,
    "RestrictPublicBuckets": boolean
  },
  "VpcConfiguration": {
    "VpcId": "string"
  }
},
"AwsS3AccountPublicAccessBlock": {
  "BlockPublicAcls": boolean,
  "BlockPublicPolicy": boolean,
  "IgnorePublicAcls": boolean,
  "RestrictPublicBuckets": boolean
},
"AwsS3Bucket": {
  "AccessControlList": "string",
  "BucketLifecycleConfiguration": {
    "Rules": [{
      "AbortIncompleteMultipartUpload": {
        "DaysAfterInitiation": number
      },
      "ExpirationDate": "string",
      "ExpirationInDays": number,
      "ExpiredObjectDeleteMarker": boolean,
      "Filter": {
        "Predicate": {
          "Operands": [{
            "Prefix": "string",
            "Type": "string"
          }
        ]
      }
    }
  ]
},

```

```

    {
      "Tag": {
        "Key": "string",
        "Value": "string"
      },
      "Type": "string"
    }
  ],
  "Type": "string"
}
},
"Id": "string",
"NoncurrentVersionExpirationInDays": number,
"NoncurrentVersionTransitions": [{
  "Days": number,
  "StorageClass": "string"
}],
"Prefix": "string",
"Status": "string",
"Transitions": [{
  "Date": "string",
  "Days": number,
  "StorageClass": "string"
}]
}]
},
"BucketLoggingConfiguration": {
  "DestinationBucketName": "string",
  "LogFilePrefix": "string"
},
"BucketName": "string",
"BucketNotificationConfiguration": {
  "Configurations": [{
    "Destination": "string",
    "Events": ["string"],
    "Filter": {
      "S3KeyFilter": {
        "FilterRules": [{
          "Name": "string",
          "Value": "string"
        }]
      }
    }
  ]
},
"Type": "string"

```



```

    ]]
  },
  "BucketVersioningConfiguration": {
    "IsMfaDeleteEnabled": boolean,
    "Status": "string"
  },
  "BucketWebsiteConfiguration": {
    "ErrorDocument": "string",
    "IndexDocumentSuffix": "string",
    "RedirectAllRequestsTo": {
      "HostName": "string",
      "Protocol": "string"
    },
  },
  "RoutingRules": [{
    "Condition": {
      "HttpErrorCodeReturnedEquals": "string",
      "KeyPrefixEquals": "string"
    },
    "Redirect": {
      "HostName": "string",
      "HttpRedirectCode": "string",
      "Protocol": "string",
      "ReplaceKeyPrefixWith": "string",
      "ReplaceKeyWith": "string"
    }
  }]
},
"CreatedAt": "string",
"ObjectLockConfiguration": {
  "ObjectLockEnabled": "string",
  "Rule": {
    "DefaultRetention": {
      "Days": integer,
      "Mode": "string",
      "Years": integer
    }
  }
},
"OwnerAccountId": "string",
"OwnerId": "string",
"OwnerName": "string",
"PublicAccessBlockConfiguration": {
  "BlockPublicAcls": boolean,
  "BlockPublicPolicy": boolean,

```

```

    "IgnorePublicAcls": boolean,
    "RestrictPublicBuckets": boolean
  },
  "ServerSideEncryptionConfiguration": {
    "Rules": [{
      "ApplyServerSideEncryptionByDefault": {
        "KMSMasterKeyID": "string",
        "SSEAlgorithm": "string"
      }
    }]
  },
  "AwsS3Object": {
    "ContentType": "string",
    "ETag": "string",
    "LastModified": "string",
    "ServerSideEncryption": "string",
    "SSEKMSKeyId": "string",
    "VersionId": "string"
  },
  "AwsSagemakerNotebookInstance": {
    "DirectInternetAccess": "string",
    "InstanceMetadataServiceConfiguration": {
      "MinimumInstanceMetadataServiceVersion": "string"
    },
    "InstanceType": "string",
    "LastModifiedTime": "string",
    "NetworkInterfaceId": "string",
    "NotebookInstanceArn": "string",
    "NotebookInstanceName": "string",
    "NotebookInstanceStatus": "string",
    "PlatformIdentifier": "string",
    "RoleArn": "string",
    "RootAccess": "string",
    "SecurityGroups": ["string"],
    "SubnetId": "string",
    "Url": "string",
    "VolumeSizeInGB": number
  },
  "AwsSecretsManagerSecret": {
    "Deleted": boolean,
    "Description": "string",
    "KmsKeyId": "string",
    "Name": "string",

```

```

    "RotationEnabled": boolean,
    "RotationLambdaArn": "string",
    "RotationOccurredWithinFrequency": boolean,
    "RotationRules": {
      "AutomaticallyAfterDays": integer
    }
  },
  "AwsSnsTopic": {
    "ApplicationSuccessFeedbackRoleArn": "string",
    "FirehoseFailureFeedbackRoleArn": "string",
    "FirehoseSuccessFeedbackRoleArn": "string",
    "HttpFailureFeedbackRoleArn": "string",
    "HttpSuccessFeedbackRoleArn": "string",
    "KmsMasterKeyId": "string",
    "Owner": "string",
    "SqsFailureFeedbackRoleArn": "string",
    "SqsSuccessFeedbackRoleArn": "string",
    "Subscription": {
      "Endpoint": "string",
      "Protocol": "string"
    },
    "TopicName": "string"
  },
  "AwsSqsQueue": {
    "DeadLetterTargetArn": "string",
    "KmsDataKeyReusePeriodSeconds": number,
    "KmsMasterKeyId": "string",
    "QueueName": "string"
  },
  "AwsSsmPatchCompliance": {
    "Patch": {
      "ComplianceSummary": {
        "ComplianceType": "string",
        "CompliantCriticalCount": integer,
        "CompliantHighCount": integer,
        "CompliantInformationalCount": integer,
        "CompliantLowCount": integer,
        "CompliantMediumCount": integer,
        "CompliantUnspecifiedCount": integer,
        "ExecutionType": "string",
        "NonCompliantCriticalCount": integer,
        "NonCompliantHighCount": integer,
        "NonCompliantInformationalCount": integer,
        "NonCompliantLowCount": integer,

```

```

        "NonCompliantMediumCount": integer,
        "NonCompliantUnspecifiedCount": integer,
        "OverallSeverity": "string",
        "PatchBaselineId": "string",
        "PatchGroup": "string",
        "Status": "string"
    }
}
},
"AwsStepFunctionStateMachine": {
    "StateMachineArn": "string",
    "Name": "string",
    "Status": "string",
    "RoleArn": "string",
    "Type": "string",
    "LoggingConfiguration": {
        "Level": "string",
        "IncludeExecutionData": boolean
    },
    "TracingConfiguration": {
        "Enabled": boolean
    }
},
"AwsWafRateBasedRule": {
    "MatchPredicates": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
    }],
    "MetricName": "string",
    "Name": "string",
    "RateKey": "string",
    "RateLimit": number,
    "RuleId": "string"
},
"AwsWafRegionalRateBasedRule": {
    "MatchPredicates": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
    }],
    "MetricName": "string",
    "Name": "string",
    "RateKey": "string",

```

```

    "RateLimit": number,
    "RuleId": "string"
  },
  "AwsWafRegionalRule": {
    "MetricName": "string",
    "Name": "string",
    "RuleId": "string",
    "PredicateList": [{
      "DataId": "string",
      "Negated": boolean,
      "Type": "string"
    }]
  },
  "AwsWafRegionalRuleGroup": {
    "MetricName": "string",
    "Name": "string",
    "RuleGroupId": "string",
    "Rules": [{
      "Action": {
        "Type": "string"
      },
      "Priority": number,
      "RuleId": "string",
      "Type": "string"
    }]
  },
  "AwsWafRegionalWebAcl": {
    "DefaultAction": "string",
    "MetricName": "string",
    "Name": "string",
    "RulesList": [{
      "Action": {
        "Type": "string"
      },
      "Priority": number,
      "RuleId": "string",
      "Type": "string",
      "ExcludedRules": [{
        "ExclusionType": "string",
        "RuleId": "string"
      }],
      "OverrideAction": {
        "Type": "string"
      }
    }]
  }
}

```

```
    }],  
    "WebAclId": "string"  
  },  
  "AwsWafRule": {  
    "MetricName": "string",  
    "Name": "string",  
    "PredicateList": [{  
      "DataId": "string",  
      "Negated": boolean,  
      "Type": "string"  
    }],  
    "RuleId": "string"  
  },  
  "AwsWafRuleGroup": {  
    "MetricName": "string",  
    "Name": "string",  
    "RuleGroupId": "string",  
    "Rules": [{  
      "Action": {  
        "Type": "string"  
      },  
      "Priority": number,  
      "RuleId": "string",  
      "Type": "string"  
    }]  
  },  
  "AwsWafv2RuleGroup": {  
    "Arn": "string",  
    "Capacity": number,  
    "Description": "string",  
    "Id": "string",  
    "Name": "string",  
    "Rules": [{  
      "Action": {  
        "Allow": {  
          "CustomRequestHandling": {  
            "InsertHeaders": [  
              {  
                "Name": "string",  
                "Value": "string"  
              },  
              {  
                "Name": "string",  
                "Value": "string"  
              }  
            ]  
          }  
        }  
      }  
    }]  
  }
```

```

    }
  ]
}
},
"Name": "string",
"Priority": number,
"VisibilityConfig": {
  "CloudWatchMetricsEnabled": boolean,
  "MetricName": "string",
  "SampledRequestsEnabled": boolean
}
}],
"VisibilityConfig": {
  "CloudWatchMetricsEnabled": boolean,
  "MetricName": "string",
  "SampledRequestsEnabled": boolean
}
},
"AwsWafWebAcl": {
  "DefaultAction": "string",
  "Name": "string",
  "Rules": [{
    "Action": {
      "Type": "string"
    },
    "ExcludedRules": [{
      "RuleId": "string"
    }],
    "OverrideAction": {
      "Type": "string"
    },
    "Priority": number,
    "RuleId": "string",
    "Type": "string"
  }],
  "WebAclId": "string"
},
"AwsWafv2WebAcl": {
  "Arn": "string",
  "Capacity": number,
  "CaptchaConfig": {
    "ImmunityTimeProperty": {
      "ImmunityTime": number
    }
  }
}

```

```

    }
  },
  "DefaultAction": {
    "Block": {}
  },
  "Description": "string",
  "ManagedbyFirewallManager": boolean,
  "Name": "string",
  "Rules": [{
    "Action": {
      "RuleAction": {
        "Block": {}
      }
    },
    "Name": "string",
    "Priority": number,
    "VisibilityConfig": {
      "SampledRequestsEnabled": boolean,
      "CloudWatchMetricsEnabled": boolean,
      "MetricName": "string"
    }
  }],
  "VisibilityConfig": {
    "SampledRequestsEnabled": boolean,
    "CloudWatchMetricsEnabled": boolean,
    "MetricName": "string"
  },
  "AwsXrayEncryptionConfig": {
    "KeyId": "string",
    "Status": "string",
    "Type": "string"
  },
  "Container": {
    "ContainerRuntime": "string",
    "ImageId": "string",
    "ImageName": "string",
    "LaunchedAt": "string",
    "Name": "string",
    "Privileged": boolean,
    "VolumeMounts": [{
      "Name": "string",
      "MountPath": "string"
    }]
  }
}

```



```
    },
    "Other": {
      "string": "string"
    },
    "Id": "string",
    "Partition": "string",
    "Region": "string",
    "ResourceRole": "string",
    "Tags": {
      "string": "string"
    },
    "Type": "string"
  ]],
  "SchemaVersion": "string",
  "Severity": {
    "Label": "string",
    "Normalized": number,
    "Original": "string"
  },
  "Sample": boolean,
  "SourceUrl": "string",
  "Threats": [{
    "FilePaths": [{
      "FileName": "string",
      "FilePath": "string",
      "Hash": "string",
      "ResourceId": "string"
    }],
    "ItemCount": number,
    "Name": "string",
    "Severity": "string"
  ]],
  "ThreatIntelIndicators": [{
    "Category": "string",
    "LastObservedAt": "string",
    "Source": "string",
    "SourceUrl": "string",
    "Type": "string",
    "Value": "string"
  ]],
  "Title": "string",
  "Types": ["string"],
  "UpdatedAt": "string",
  "UserDefinedFields": {
```

```

    "string": "string"
  },
  "VerificationState": "string",
  "Vulnerabilities": [{
    "CodeVulnerabilities": [{
      "Cwes": [
        "string",
        "string"
      ],
      "FilePath": {
        "EndLine": integer,
        "FileName": "string",
        "FilePath": "string",
        "StartLine": integer
      },
      "SourceArn": "string"
    }],
    "Cvss": [{
      "Adjustments": [{
        "Metric": "string",
        "Reason": "string"
      }],
      "BaseScore": number,
      "BaseVector": "string",
      "Source": "string",
      "Version": "string"
    }],
    "EpssScore": number,
    "ExploitAvailable": "string",
    "FixAvailable": "string",
    "Id": "string",
    "LastKnownExploitAt": "string",
    "ReferenceUrls": ["string"],
    "RelatedVulnerabilities": ["string"],
    "Vendor": {
      "Name": "string",
      "Url": "string",
      "VendorCreatedAt": "string",
      "VendorSeverity": "string",
      "VendorUpdatedAt": "string"
    },
    "VulnerablePackages": [{
      "Architecture": "string",
      "Epoch": "string",

```

```

    "FilePath": "string",
    "FixedInVersion": "string",
    "Name": "string",
    "PackageManager": "string",
    "Release": "string",
    "Remediation": "string",
    "SourceLayerArn": "string",
    "SourceLayerHash": "string",
    "Version": "string"
  ]
}],
  "Workflow": {
    "Status": "string"
  },
  "WorkflowState": "string"
}
]

```

Impacto de la consolidación en los campos y valores ASFF

AWS Security Hub Cloud Security Posture Management (CSPM) ofrece dos tipos de consolidación de los controles:

- **Vista de controles consolidada:** con este tipo de consolidación, cada control tiene un identificador único en todos los estándares. Además, en la consola CSPM de Security Hub, la página Controles muestra todos los controles de todos los estándares.
- **Resultados de control consolidados:** con este tipo de consolidación, Security Hub CSPM produce un único hallazgo para un control, incluso si el control se aplica a varios estándares habilitados. Esto puede reducir el ruido de detección.

No puede activar ni desactivar la vista de controles consolidados. Los hallazgos de control consolidados están habilitados de forma predeterminada si habilita el CSPM de Security Hub a partir del 23 de febrero de 2023. De lo contrario, está desactivado de forma predeterminada. Sin embargo, en el caso de las organizaciones, los hallazgos de control consolidados solo están habilitados para las cuentas de los miembros del CSPM de Security Hub si están habilitados para la cuenta de administrador. Para obtener más información sobre los hallazgos del control consolidado, consulte.

[Generación y actualización de los resultados de control](#)

Ambos tipos de consolidación afectan a los campos y valores de los hallazgos de control en el [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

Temas

- [Vista de controles consolidada: cambios en ASFF](#)
- [Resultados de control consolidados: cambios en ASFF](#)
- [Generador IDs de resultados de control consolidados antes y después](#)
- [Cómo afecta la consolidación al control IDs y a los títulos](#)
- [Actualización de los flujos de trabajo para la consolidación](#)

Vista de controles consolidada: cambios en ASFF

La función de vista de controles consolidada introdujo los siguientes cambios en los campos y valores de los hallazgos de control del ASFF. Si sus flujos de trabajo no se basan en los valores de estos campos de ASFF, no es necesario realizar ninguna acción. Si tiene flujos de trabajo que se basan en valores específicos para estos campos, actualice sus flujos de trabajo para usar los valores actuales.

Campo de ASFF	Valor de muestra antes de la vista de controles consolidados	Ejemplo de valor después de una vista de controles consolidada y una descripción del cambio
Conformidad. SecurityControlId	No aplicable (campo nuevo)	EC22. Introduzca un único identificador de control en todos los estándares. <code>ProductFields.RuleId</code> sigue proporcionando el identificador de control estándar para los controles CIS v1.2.0. <code>ProductFields.ControlId</code> sigue proporcionando el identificador de control basado en estándares para los controles de otros estándares.

Campo de ASFF	Valor de muestra antes de la vista de controles consolidados	Ejemplo de valor después de una vista de controles consolidada y una descripción del cambio
Cumplimiento. Associate Standards	No aplicable (campo nuevo)	[{" StandardsId ":" standards /aws-foundational-security-best-practices/v /1.0.0 «}] Muestra en qué estándares está activado un control.
ProductFields. ArchivalReasons. -----SEP-----:0/Descripción	No aplicable (campo nuevo)	“El resultado se encuentra ARCHIVADO porque los resultados del control consolidado se han activado o desactivado. Esto hace que los resultados del estado anterior se archiven cuando se generen nuevos resultados”. Describe por qué Security Hub CSPM ha archivado las conclusiones existentes.
ProductFields. ArchivalReasons. -----sep-----:0/ReasonCode	No aplicable (campo nuevo)	“CONSOLIDATED_CONTROL_FINDINGS_UPDATE” Proporciona el motivo por el que Security Hub CSPM ha archivado las conclusiones existentes.

Campo de ASFF	Valor de muestra antes de la vista de controles consolidados	Ejemplo de valor después de una vista de controles consolidada y una descripción del cambio
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Este campo ya no hace referencia a un estándar.
Remediation.Recommendation.Text	«Para obtener instrucciones sobre cómo solucionar este problema, consulte la documentación PCI DSS de AWS Security Hub Cloud Security Posture Management (CSPM)».	«Para obtener instrucciones sobre cómo corregir este problema, consulte la documentación de controles de AWS Security Hub Cloud Security Posture Management (CSPM)». Este campo ya no hace referencia a un estándar.
Remediation.Recommendation.Url	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Este campo ya no hace referencia a un estándar.

Resultados de control consolidados: cambios en ASFF

Si habilita los resultados de control consolidados, es posible que se vea afectado por los siguientes cambios en los campos y valores de los hallazgos de control del ASFF. Estos cambios se suman a los cambios introducidos por la función de visualización de controles consolidados. Si sus flujos de trabajo no se basan en los valores de estos campos ASFF, no es necesario realizar ninguna acción. Si tiene flujos de trabajo que se basan en valores específicos para estos campos, actualice sus flujos de trabajo para usar los valores actuales.

Tip

Si utiliza la solución [Automated Security Response en la AWS versión 2.0.0](#), tenga en cuenta que respalda los resultados de control consolidados. Esto significa que puede mantener sus flujos de trabajo actuales si habilita los resultados de control consolidados.

Campo de ASFF	Pruebe el valor antes de habilitar los hallazgos de control consolidados	Ejemplo de valor después de habilitar los resultados de control consolidados y una descripción del cambio
GeneratorId	aws-foundational-security-best-practices/v/1.0.0/Config 1.	security-control/Config.1 Este campo ya no hace referencia a un estándar.
Título	PCI.config.1 debe estar activado AWS Config	AWS Config debe estar activado Este campo ya no hace referencia a información específica del estándar.
Id	arn:aws:securityhub:eu-central-1:123456789012:6d6a26-a156-48f0-9403-115983e5a956 subscription/pci-dss/v/3.2.1/PCI.IAM.5/finding/ab	arn:aws:securityhub: eu-central-1:123456789012: security - 6d6a26-a156-48f0-9403-115983e5a956 control/iam.9/finding/ab Este campo ya no hace referencia a un estándar.
ProductFields.ControlId	PCI. EC22.	Eliminado. En su lugar, consulte Compliance.SecurityControlId . Este campo se ha eliminado en favor de un único identificador

Campo de ASFF	Pruebe el valor antes de habilitar los hallazgos de control consolidados	Ejemplo de valor después de habilitar los resultados de control consolidados y una descripción del cambio
		de control independiente del estándar.
ProductFields.RuleId	1.3	Eliminado. En su lugar, consulte <code>Compliance.SecurityControlId</code>. Este campo se ha eliminado en favor de un único identificador de control independiente del estándar.
Descripción	Este control PCI DSS comprueba si AWS Config está activado en la cuenta corriente y en la región.	Este AWS control comprueba si AWS Config está activado en la cuenta corriente y la región. Este campo ya no hace referencia a un estándar.
Gravedad	<pre> "Severity": { "Product": 90, "Label": "CRÍTICO", "Normalized": 90, "Original": "CRÍTICO" } </pre>	<pre> "Severity": { "Label": "CRÍTICO", "Normalized": 90, "Original": "CRÍTICO" } </pre> Security Hub CSPM ya no utiliza el campo <code>Producto</code> para describir la gravedad de un hallazgo.

Campo de ASFF	Pruebe el valor antes de habilitar los hallazgos de control consolidados	Ejemplo de valor después de habilitar los resultados de control consolidados y una descripción del cambio
Tipos	["Software, configuración Checks/ Industry y normas reglamentarias/PCI-DSS"]	["Software, configuración y normas reglamentarias"] Checks/ Industry Este campo ya no hace referencia a un estándar.
Conformidad. RelatedRequirements	["PCI DSS 10.5.2", "PCI DSS 11.5", « AWS Fundamentos de la CEI 2.5"]	["PCI DSS v3.2.1/10.5.2", "PCI DSS v3.2.1/11.5", «Índice de referencia sobre AWS fundaciones de la CEI [v1.2.0/2.5"] Este campo muestra los requisitos relacionados en todos los estándares habilitados.
CreatedAt	2022-05-05T08:18:13.138Z	2022-09-25T08:18:13.138Z El formato sigue siendo el mismo, pero el valor se restablece cuando se habilitan las conclusiones de control consolidadas.
FirstObservedAt	2022-05-07T08:18:13.138Z	2022-09-28T08:18:13.138Z El formato sigue siendo el mismo, pero el valor se restablece cuando se habilitan las conclusiones de control consolidadas.

Campo de ASFF	Pruebe el valor antes de habilitar los hallazgos de control consolidados	Ejemplo de valor después de habilitar los resultados de control consolidados y una descripción del cambio
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation	Eliminado. En su lugar, consulte <code>Remediation.Recommendation.Url</code> .
ProductFields.StandardsArn	<code>arn:aws:securityhub:::/1.0.0/standards/aws-foundational-security-best-practices/v</code>	Eliminado. En su lugar, consulte <code>Compliance.AssociatedStandards</code> .
ProductFields.StandardsControlArn	<code>arn:aws:securityhub:us-east-1:123456789012:1control/aws-foundational-security-best-practices/v/1.0.0/Config.</code>	Eliminado. Security Hub CSPM genera un resultado para una comprobación de seguridad en todos los estándares.
ProductFields.StandardsGuideArn	<code>arn:aws:securityhub:::/1.2.0/ruleset/cis-aws-foundations-benchmark/v</code>	Eliminado. En su lugar, consulte <code>Compliance.AssociatedStandards</code> .
ProductFields.StandardsGuideSubscriptionArn	<code>arn:aws:securityhub:us-east-2:123456789012:/1.2.0 subscription/cis-aws-foundations-benchmark/v</code>	Eliminado. Security Hub CSPM genera un resultado para una comprobación de seguridad en todos los estándares.
ProductFields.StandardsSubscriptionArn	<code>arn:aws:securityhub:us-east-1:123456789012:/1.0.0 subscription/aws-foundational-security-best-practices/v</code>	Eliminado. Security Hub CSPM genera un resultado para una comprobación de seguridad en todos los estándares.

Campo de ASFF	Pruebe el valor antes de habilitar los hallazgos de control consolidados	Ejemplo de valor después de habilitar los resultados de control consolidados y una descripción del cambio
ProductFields.aws/securityhub/FindingId	arn:aws:securityhub:us-east-1::/751c2173-7372-4e12-8656-a5210dfb1d67 product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0/Config.1/finding	arn:aws:securityhub: us-east-1 :: /751c2173-7372-4e12-8656-a5210dfb1d67 product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/Config.1/finding Este campo ya no hace referencia a un estándar.

Valores para los campos del ASFF proporcionados por el cliente tras activar los resultados de control consolidados

Si habilita los hallazgos de control consolidados, Security Hub CSPM genera un hallazgo para todos los estándares y archiva los hallazgos originales (hallazgos separados para cada estándar).

Las actualizaciones que haya realizado en los hallazgos originales mediante la consola CSPM de Security Hub o la [BatchUpdateFindings](#) operación no se conservarán en los nuevos hallazgos. Si es necesario, puede recuperar estos datos consultando los hallazgos archivados. Para revisar los hallazgos archivados, puede usar la página Hallazgos de la consola CSPM de Security Hub y configurar el filtro de estado del registro en ARCHIVADO. Como alternativa, puede utilizar el [GetFindings](#) funcionamiento de la API CSPM de Security Hub.

Campo de ASFF proporcionado por el cliente	Descripción del cambio tras habilitar los resultados de control consolidados
Confianza	Se restablece al estado vacío.
Criticidad	Se restablece al estado vacío.
Nota	Se restablece al estado vacío.
RelatedFindings	Se restablece al estado vacío.

Campo de ASFF proporcionado por el cliente	Descripción del cambio tras habilitar los resultados de control consolidados
Gravedad	Gravedad predeterminada del resultado (coincide con la gravedad del control).
Tipos	Se restablece a un valor independiente del estándar.
UserDefinedFields	Se restablece al estado vacío.
VerificationState	Se restablece al estado vacío.
Flujo de trabajo	Los nuevos resultados fallidos tienen un valor predeterminado de NEW. Los nuevos resultados aprobados tienen un valor predeterminado de RESOLVED.

Generador IDs de resultados de control consolidados antes y después

La siguiente tabla muestra los cambios en los valores de ID del generador para los controles cuando se habilitan los hallazgos de control consolidados. Estos cambios se aplican a los controles que Security Hub CSPM admitía a partir del 15 de febrero de 2023.

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
arn:aws:securityhub::: /1.1 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	control de seguridad/ CloudWatch .1
arn:aws:securityhub::: /1.10 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/IAM.16
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /1.11	security-control/IAM.17
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /1.12	security-control/IAM.4

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /1.13	security-control/IAM.9
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /1.14	security-control/IAM.6
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /1.16	security-control/IAM.2
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /1.2	security-control/IAM.5
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /1.20	security-control/IAM.18
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /1.22	security-control/IAM.1
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /1.3	security-control/IAM.8
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /1.4	security-control/IAM.3
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /1.5	security-control/IAM.11
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /1.6	security-control/IAM.12
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /1.7	security-control/IAM.13
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /1.8	security-control/IAM.14

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /1.9	security-control/IAM.15
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /2.1	control de seguridad/ CloudTrail .1
arn:aws:securityhub::: /2.2 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ 4CloudTrail.
arn:aws:securityhub::: /2.3 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ 6CloudTrail.
arn:aws:securityhub::: /2.4 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ 5CloudTrail.
arn:aws:securityhub::: /2.5 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/Config.1
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /2.6	security-control/ 7CloudTrail.
arn:aws:securityhub::: /2.7 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ 2CloudTrail.
arn:aws:securityhub::: /2.8 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/KMS.4
arn:aws:securityhub::: ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule /2.9	security-control/ 6EC2.
arn:aws:securityhub::: /3.1 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ 2CloudWatch.
arn:aws:securityhub::: /3.2 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	control-seguridad/ 3CloudWatch.

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
arn:aws:securityhub::: /3.3 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	control de seguridad/ 1CloudWatch.
arn:aws:securityhub::: /3.4 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ 4CloudWatch.
arn:aws:securityhub::: /3.5 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ 5CloudWatch.
arn:aws:securityhub::: /3.6 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ 6CloudWatch.
arn:aws:securityhub::: /3.7 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ 7CloudWatch.
arn:aws:securityhub::: /3.8 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ CloudWatch .8
arn:aws:securityhub::: /3.9 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ 9CloudWatch.
arn:aws:securityhub::: /3.10 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ CloudWatch .10
arn:aws:securityhub::: /3.11 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ CloudWatch 1.1
arn:aws:securityhub::: /3.12 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ CloudWatch .12
arn:aws:securityhub::: /3.13 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ CloudWatch .13
arn:aws:securityhub::: /3.14 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ CloudWatch .14

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
arn:aws:securityhub:::/4.1 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ EC2 .13
arn:aws:securityhub:::/4.2 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ EC2 .14
arn:aws:securityhub:::/4.3 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ 2EC2.
cis-aws-foundations-benchmark/v/1.4.0/1.10	security-control/IAM.5
cis-aws-foundations-benchmark/v/1.4.0/1,14	security-control/IAM.3
cis-aws-foundations-benchmark/v/1.4.0/1,16	security-control/IAM.1
cis-aws-foundations-benchmark/v/1.4.0/1,17	security-control/IAM.18
cis-aws-foundations-benchmark/v/1.4.0/1.4	security-control/IAM.4
cis-aws-foundations-benchmark/v/1.4.0/1.5	security-control/IAM.9
cis-aws-foundations-benchmark/v/1.4.0/1.6	security-control/IAM.6
cis-aws-foundations-benchmark/v/1.4.0/1.7	control de seguridad/ .1 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/1.8	security-control/IAM.15
cis-aws-foundations-benchmark/v/1.4.0/1.9	security-control/IAM.16
cis-aws-foundations-benchmark/v/1.4.0/2.1.2	security-control/S3.5
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.1	security-control/S3.1
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.2	security-control/S3.8
cis-aws-foundations-benchmark/v/1.4.0/2.2.1	control de seguridad/ 7. EC2
cis-aws-foundations-benchmark/v/1.4.0/2.3.1	security-control/RDS.3

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
cis-aws-foundations-benchmark/v/1.4.0/3.1	control de seguridad/ .1 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.2	control de seguridad/ 4CloudTrail.
cis-aws-foundations-benchmark/v/1.4.0/3.4	control de seguridad/ 5. CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.5	security-control/Config.1
cis-aws-foundations-benchmark/v/1.4.0/3.6	security-control/S3.9
cis-aws-foundations-benchmark/v/1.4.0/3.7	control de seguridad/ .2 CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.8	security-control/KMS.4
cis-aws-foundations-benchmark/v/1.4.0/3.9	control de seguridad/ 6. EC2
cis-aws-foundations-benchmark/v/1.4.0/4.3	control de seguridad/ .1 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.4	control de seguridad/ 4CloudWatch.
cis-aws-foundations-benchmark/v/1.4.0/4.5	control de seguridad/ 5. CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.6	control de seguridad/ 6. CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.7	control de seguridad/ 7. CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.8	control de seguridad/ .8 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.9	control de seguridad/ .9 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.10	control de seguridad/ .10 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.11	control de seguridad/ 1.1 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.12	control de seguridad/ 1.2 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.13	control de seguridad/ 1.3 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.14	control de seguridad/ .14 CloudWatch

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
cis-aws-foundations-benchmark/v/1.4.0/5.1	control de seguridad/ 2.1 EC2
cis-aws-foundations-benchmark/v/1.4.0/5.3	control de seguridad/ .2 EC2
aws-foundational-security-best- 1practices/ v/1.0.0/Account.	security-control/Account.1
aws-foundational-security-best- practices/ v/1.0.0/ACM 1.	security-control/ACM.1
aws-foundational-security-best- practices/ v/1.0.0/APIGateway 1.	control de seguridad/ .1 APIGateway
aws-foundational-security-best- 2practices/ v/1.0.0/APIGateway.	control de seguridad/ .2 APIGateway
aws-foundational-security-best- 3practices/ v/1.0.0/APIGateway.	control de seguridad/ 3APIGateway.
aws-foundational-security-best- 4practices/ v/1.0.0/APIGateway.	control de seguridad/ .4APIGateway.
aws-foundational-security-best- 5practices/ v/1.0.0/APIGateway.	control de seguridad/ .5 APIGateway
aws-foundational-security-best- 8practices/ v/1.0.0/APIGateway.	control de seguridad/ .8 APIGateway
aws-foundational-security-best- 9practices/ v/1.0.0/APIGateway.	control de seguridad/ .9 APIGateway
aws-foundational-security-best- 1practices/ v/1.0.0/AutoScaling.	control de seguridad/ .1 AutoScaling
aws-foundational-security-best- 2practices/ v/1.0.0/AutoScaling.	control de seguridad/ .2 AutoScaling

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
aws-foundational-security-best- 3practices/ v/1.0.0/AutoScaling.	control de seguridad/ 3AutoScaling.
aws-foundational-security-best- 5practices/ v/1.0.0/Autoscaling.	security-control/Autoscaling.5
aws-foundational-security-best- 6practices/ v/1.0.0/AutoScaling.	control de seguridad/ .6 AutoScaling
aws-foundational-security-best- 9practices/ v/1.0.0/AutoScaling.	control de seguridad/ .9 AutoScaling
aws-foundational-security-best- 1practices/ v/1.0.0/CloudFront.	control de seguridad/ .1 CloudFront
aws-foundational-security-best- 3practices/ v/1.0.0/CloudFront.	control de seguridad/ 3CloudFront.
aws-foundational-security-best- 4practices/ v/1.0.0/CloudFront.	control de seguridad/ .4CloudFront.
aws-foundational-security-best- 5practices/ v/1.0.0/CloudFront.	control de seguridad/ .5 CloudFront
aws-foundational-security-best- 6practices/ v/1.0.0/CloudFront.	control de seguridad/ .6 CloudFront
aws-foundational-security-best- 7practices/ v/1.0.0/CloudFront.	control de seguridad/ .7 CloudFront
aws-foundational-security-best- 8practices/ v/1.0.0/CloudFront.	control de seguridad/ .8 CloudFront
aws-foundational-security-best- 9practices/ v/1.0.0/CloudFront.	control de seguridad/ .9 CloudFront

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
aws-foundational-security-best-practices/v/1.0.0/CloudFront 1.0	control de seguridad/ .10 CloudFront
aws-foundational-security-best-practices/v/1.0.0/CloudFront 1.2	control de seguridad/ .12 CloudFront
aws-foundational-security-best-1practices/v/1.0.0/CloudTrail.	control de seguridad/ .1 CloudTrail
aws-foundational-security-best-2practices/v/1.0.0/CloudTrail.	control de seguridad/ .2 CloudTrail
aws-foundational-security-best-4practices/v/1.0.0/CloudTrail.	control de seguridad/ .4CloudTrail.
aws-foundational-security-best-5practices/v/1.0.0/CloudTrail.	control de seguridad/ .5 CloudTrail
aws-foundational-security-best-1practices/v/1.0.0/CodeBuild.	control de seguridad/ .1 CodeBuild
aws-foundational-security-best-2practices/v/1.0.0/CodeBuild.	control de seguridad/ .2 CodeBuild
aws-foundational-security-best-3practices/v/1.0.0/CodeBuild.	control de seguridad/ 3CodeBuild.
aws-foundational-security-best-4practices/v/1.0.0/CodeBuild.	control de seguridad/ .4CodeBuild.
aws-foundational-security-best-1practices/v/1.0.0/Config.	security-control/Config.1
aws-foundational-security-best-practices/v/1.0.0/DMS 1.	security-control/DMS.1

GeneratorID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
aws-foundational-security-best-practices/v/1.0.0/DynamoDB 1.	security-control/DynamoDB.1
aws-foundational-security-best-practices/v/1.0.0/DynamoDB 2.	security-control/DynamoDB.2
aws-foundational-security-best-practices/v/1.0.0/DynamoDB 3.	security-control/DynamoDB.3
aws-foundational-security-best-practices/v/1.0.0/EC 2.1	control de seguridad/ .1 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.3	control de seguridad/ 3EC2.
aws-foundational-security-best-practices/v/1.0.0/EC 2.4	control de seguridad/ 4EC2.
aws-foundational-security-best-practices/v/1.0.0/EC 2.6	control de seguridad/ 6EC2.
aws-foundational-security-best-practices/v/1.0.0/EC 2.7	control de seguridad/ 7EC2.
aws-foundational-security-best-practices/v/1.0.0/EC 2.8	control de seguridad/ 8EC2.
aws-foundational-security-best-practices/v/1.0.0/EC 2.9	control de seguridad/ 9EC2.
aws-foundational-security-best-practices/v/1.0.0/EC 2.10	control de seguridad/ .10 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.15	control de seguridad/ .15 EC2

GeneratorID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
aws-foundational-security-best-practices/v/1.0.0/EC 2.16	control de seguridad/ 1.6 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.17	control de seguridad/ 1.7 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.18	control de seguridad/ .18 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.19	control de seguridad/ .19 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.2	control de seguridad/ 2EC2.
aws-foundational-security-best-practices/v/1.0.0/EC 2.20	control de seguridad/ .20 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.21	control de seguridad/ 2.1 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.23	control de seguridad/ 2.3 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.24	control de seguridad/ 2.4 EC2
aws-foundational-security-best-practices/v/1.0.0/EC 2.25	control de seguridad/ .25 EC2
aws-foundational-security-best-practices/v/1.0.0/ECR.	security-control/ECR.1
aws-foundational-security-best-practices/v/1.0.0/ECR 2.	security-control/ECR.2

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
aws-foundational-security-best-practices/v/1.0.0/ECR 3.	security-control/ECR.3
aws-foundational-security-best-practices/v/1.0.0/ECS 1.	security-control/ECS.1
aws-foundational-security-best-practices/v/1.0.0/ECS 1.0	security-control/ECS.10
aws-foundational-security-best-practices/v/1.0.0/ECS .12 practices/	security-control/ECS.12
aws-foundational-security-best-practices/v/1.0.0/ECS. 2practices/	security-control/ECS.2
aws-foundational-security-best-practices/v/1.0.0/ECS 3.	security-control/ECS.3
aws-foundational-security-best-practices/v/1.0.0/ECS. 4practices/	security-control/ECS.4
aws-foundational-security-best-practices/v/1.0.0/ECS. 5practices/	security-control/ECS.5
aws-foundational-security-best-practices/v/1.0.0/ECS. 8practices/	security-control/ECS.8
aws-foundational-security-best-practices/v/1.0.0/EFS. 1practices/	security-control/EFS.1
aws-foundational-security-best-practices/v/1.0.0/EFS 2.	security-control/EFS.2
aws-foundational-security-best-practices/v/1.0.0/EFS 3.	security-control/EFS.3

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
aws-foundational-security-best- 4practices/ v/1.0.0/EFS.	security-control/EFS.4
aws-foundational-security-best- 2practices/ v/1.0.0/EKS.	security-control/EKS.2
aws-foundational-security-best- practices/ v/1.0.0/ElasticBeanstalk 1.	control de seguridad/ .1 ElasticBeanstalk
aws-foundational-security-best- 2practices/ v/1.0.0/ElasticBeanstalk.	control de seguridad/ .2 ElasticBeanstalk
aws-foundational-security-best- practices/ v/1.0.0/ELBv 2.1	security-control/ELB.1
aws-foundational-security-best- practices/ v/1.0.0/ELB 2.	security-control/ELB.2
aws-foundational-security-best- practices/ v/1.0.0/ELB 3.	security-control/ELB.3
aws-foundational-security-best- 4practices/ v/1.0.0/ELB.	security-control/ELB.4
aws-foundational-security-best- 5practices/ v/1.0.0/ELB.	security-control/ELB.5
aws-foundational-security-best- 6practices/ v/1.0.0/ELB.	security-control/ELB.6
aws-foundational-security-best- 7practices/ v/1.0.0/ELB.	security-control/ELB.7
aws-foundational-security-best- 8practices/ v/1.0.0/ELB.	security-control/ELB.8

GeneratorID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
aws-foundational-security-best- 9practices/ v/1.0.0/ELB.	security-control/ELB.9
aws-foundational-security-best- .10 practices/ v/1.0.0/ELB	security-control/ELB.10
aws-foundational-security-best- .11 practices/ v/1.0.0/ELB	security-control/ELB.11
aws-foundational-security-best- 1.2 practices/ v/1.0.0/ELB	security-control/ELB.12
aws-foundational-security-best- 1.3 practices/ v/1.0.0/ELB	security-control/ELB.13
aws-foundational-security-best- 1.4 practices/ v/1.0.0/ELB	security-control/ELB.14
aws-foundational-security-best- 1practices/ v/1.0.0/EMR.	security-control/EMR.1
aws-foundational-security-best- practices/ v/1.0.0/ES 1.	security-control/ES.1
aws-foundational-security-best- practices/ v/1.0.0/ES 2.	security-control/ES.2
aws-foundational-security-best- practices/ v/1.0.0/ES 3.	security-control/ES.3
aws-foundational-security-best- 4practices/ v/1.0.0/ES.	security-control/ES.4
aws-foundational-security-best- 5practices/ v/1.0.0/ES.	security-control/ES.5

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
aws-foundational-security-best- 6practices/ v/1.0.0/ES.	security-control/ES.6
aws-foundational-security-best- 7practices/ v/1.0.0/ES.	security-control/ES.7
aws-foundational-security-best- 8practices/ v/1.0.0/ES.	security-control/ES.8
aws-foundational-security-best- 1practices/ v/1.0.0/GuardDuty.	control de seguridad/ .1 GuardDuty
aws-foundational-security-best- practices/ v/1.0.0/IAM 1.	security-control/IAM.1
aws-foundational-security-best- practices/ v/1.0.0/IAM 2.	security-control/IAM.2
aws-foundational-security-best- practices/ v/1.0.0/IAM 2.1	security-control/IAM.21
aws-foundational-security-best- 3practices/ v/1.0.0/IAM.	security-control/IAM.3
aws-foundational-security-best- 4practices/ v/1.0.0/IAM.	security-control/IAM.4
aws-foundational-security-best- 5practices/ v/1.0.0/IAM.	security-control/IAM.5
aws-foundational-security-best- 6practices/ v/1.0.0/IAM.	security-control/IAM.6
aws-foundational-security-best- 7practices/ v/1.0.0/IAM.	security-control/IAM.7

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
aws-foundational-security-best- 8practices/ v/1.0.0/IAM.	security-control/IAM.8
aws-foundational-security-best- 1practices/ v/1.0.0/Kinesis.	security-control/Kinesis.1
aws-foundational-security-best- practices/ v/1.0.0/KMS 1.	security-control/KMS.1
aws-foundational-security-best- practices/ v/1.0.0/KMS 2.	security-control/KMS.2
aws-foundational-security-best- practices/ v/1.0.0/KMS 3.	security-control/KMS.3
aws-foundational-security-best- practices/ v/1.0.0/Lambda 1.	security-control/Lambda.1
aws-foundational-security-best- practices/ v/1.0.0/Lambda 2.	security-control/Lambda.2
aws-foundational-security-best- 5practices/ v/1.0.0/Lambda.	security-control/Lambda.5
aws-foundational-security-best- 3practices/ v/1.0.0/NetworkFirewall.	control de seguridad/ 3NetworkFirewall.
aws-foundational-security-best- 4practices/ v/1.0.0/NetworkFirewall.	control de seguridad/ .4NetworkFirewall.
aws-foundational-security-best- 5practices/ v/1.0.0/NetworkFirewall.	control de seguridad/ .5 NetworkFirewall
aws-foundational-security-best- 6practices/ v/1.0.0/NetworkFirewall.	control de seguridad/ .6 NetworkFirewall

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
aws-foundational-security-best- 1practices/ v/1.0.0/Opensearch.	security-control/Opensearch.1
aws-foundational-security-best- practices/ v/1.0.0/Opensearch 2.	security-control/Opensearch.2
aws-foundational-security-best- practices/ v/1.0.0/Opensearch 3.	security-control/Opensearch.3
aws-foundational-security-best- 4practices/ v/1.0.0/Opensearch.	security-control/Opensearch.4
aws-foundational-security-best- 5practices/ v/1.0.0/Opensearch.	security-control/Opensearch.5
aws-foundational-security-best- 6practices/ v/1.0.0/Opensearch.	security-control/Opensearch.6
aws-foundational-security-best- 7practices/ v/1.0.0/Opensearch.	security-control/Opensearch.7
aws-foundational-security-best- 8practices/ v/1.0.0/Opensearch.	security-control/Opensearch.8
aws-foundational-security-best- 1practices/ v/1.0.0/RDS.	security-control/RDS.1
aws-foundational-security-best- practices/ v/1.0.0/RDS 1.0	security-control/RDS.10
aws-foundational-security-best- .11 practices/ v/1.0.0/RDS	security-control/RDS.11
aws-foundational-security-best- 1.2 practices/ v/1.0.0/RDS	security-control/RDS.12

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
aws-foundational-security-best- 1.3 practices/ v/1.0.0/RDS	security-control/RDS.13
aws-foundational-security-best- 1.4 practices/ v/1.0.0/RDS	security-control/RDS.14
aws-foundational-security-best- 1.5 practices/ v/1.0.0/RDS	security-control/RDS.15
aws-foundational-security-best- 1.6 practices/ v/1.0.0/RDS	security-control/RDS.16
aws-foundational-security-best- 1.7 practices/ v/1.0.0/RDS	security-control/RDS.17
aws-foundational-security-best- 1.9 practices/ v/1.0.0/RDS	security-control/RDS.19
aws-foundational-security-best- 2practices/ v/1.0.0/RDS.	security-control/RDS.2
aws-foundational-security-best- practices/ v/1.0.0/RDS 2,0	security-control/RDS.20
aws-foundational-security-best- 2.1 practices/ v/1.0.0/RDS	security-control/RDS.21
aws-foundational-security-best- .22 practices/ v/1.0.0/RDS	security-control/RDS.22
aws-foundational-security-best- 2.3 practices/ v/1.0.0/RDS	security-control/RDS.23
aws-foundational-security-best- .24 practices/ v/1.0.0/RDS	security-control/RDS.24

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
aws-foundational-security-best- .25 practices/ v/1.0.0/RDS	security-control/RDS.25
aws-foundational-security-best- 3practices/ v/1.0.0/RDS.	security-control/RDS.3
aws-foundational-security-best- 4practices/ v/1.0.0/RDS.	security-control/RDS.4
aws-foundational-security-best- 5practices/ v/1.0.0/RDS.	security-control/RDS.5
aws-foundational-security-best- 6practices/ v/1.0.0/RDS.	security-control/RDS.6
aws-foundational-security-best- 7practices/ v/1.0.0/RDS.	security-control/RDS.7
aws-foundational-security-best- 8practices/ v/1.0.0/RDS.	security-control/RDS.8
aws-foundational-security-best- 9practices/ v/1.0.0/RDS.	security-control/RDS.9
aws-foundational-security-best- 1practices/ v/1.0.0/Redshift.	security-control/Redshift.1
aws-foundational-security-best- practices/ v/1.0.0/Redshift 2.	security-control/Redshift.2
aws-foundational-security-best- practices/ v/1.0.0/Redshift 3.	security-control/Redshift.3
aws-foundational-security-best- 4practices/ v/1.0.0/Redshift.	security-control/Redshift.4

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
aws-foundational-security-best- 6practices/ v/1.0.0/Redshift.	security-control/Redshift.6
aws-foundational-security-best- 7practices/ v/1.0.0/Redshift.	security-control/Redshift.7
aws-foundational-security-best- 8practices/ v/1.0.0/Redshift.	security-control/Redshift.8
aws-foundational-security-best- 9practices/ v/1.0.0/Redshift.	security-control/Redshift.9
aws-foundational-security-best- 3.1 practices/ v/1.0.0/S	security-control/S3.1
aws-foundational-security-best- practices/ v/1.0.0/S 3.12	security-control/S3.12
aws-foundational-security-best- 3,13 practices/ v/1.0.0/S	security-control/S3.13
aws-foundational-security-best- 3.2 practices/ v/1.0.0/S	security-control/S3.2
aws-foundational-security-best- practices/ v/1.0.0/S 3.3	security-control/S3.3
aws-foundational-security-best- practices/ v/1.0.0/S 3.5	security-control/S3.5
aws-foundational-security-best- practices/ v/1.0.0/S 3.6	security-control/S3.6
aws-foundational-security-best- practices/ v/1.0.0/S 3.8	security-control/S3.8

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
aws-foundational-security-best-practices/v/1.0.0/S 3.9	security-control/S3.9
aws-foundational-security-best-practices/v/1.0.0/SageMaker 1.	control de seguridad/ .1 SageMaker
aws-foundational-security-best- 2practices/v/1.0.0/SageMaker.	control de seguridad/ .2 SageMaker
aws-foundational-security-best- 3practices/v/1.0.0/SageMaker.	control de seguridad/ 3SageMaker.
aws-foundational-security-best- 1practices/v/1.0.0/SecretsManager.	control de seguridad/ .1 SecretsManager
aws-foundational-security-best- 2practices/v/1.0.0/SecretsManager.	control de seguridad/ .2 SecretsManager
aws-foundational-security-best- 3practices/v/1.0.0/SecretsManager.	control de seguridad/ 3SecretsManager.
aws-foundational-security-best- 4practices/v/1.0.0/SecretsManager.	control de seguridad/ .4SecretsManager.
aws-foundational-security-best- 1practices/v/1.0.0/SQS.	security-control/SQS.1
aws-foundational-security-best-practices/v/1.0.0/SSM 1.	security-control/SSM.1
aws-foundational-security-best-practices/v/1.0.0/SSM 2.	security-control/SSM.2
aws-foundational-security-best-practices/v/1.0.0/SSM 3.	security-control/SSM.3

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
aws-foundational-security-best- 4practices/ v/1.0.0/SSM.	security-control/SSM.4
aws-foundational-security-best- 1practices/ v/1.0.0/WAF.	security-control/WAF.1
aws-foundational-security-best- practices/ v/1.0.0/WAF 2.	security-control/WAF.2
aws-foundational-security-best- practices/ v/1.0.0/WAF 3.	security-control/WAF.3
aws-foundational-security-best- 4practices/ v/1.0.0/WAF.	security-control/WAF.4
aws-foundational-security-best- 6practices/ v/1.0.0/WAF.	security-control/WAF.6
aws-foundational-security-best- 7practices/ v/1.0.0/WAF.	security-control/WAF.7
aws-foundational-security-best- 8practices/ v/1.0.0/WAF.	security-control/WAF.8
aws-foundational-security-best- .10 practices/ v/1.0.0/WAF	security-control/WAF.10
pci-. dss/v/3.2.1/PCI AutoScaling1.	control de seguridad/ 1AutoScaling.
pci-. dss/v/3.2.1/PCI CloudTrail1.	control de seguridad/ 2CloudTrail.
pci-. dss/v/3.2.1/PCI CloudTrail2.	control de seguridad/ 3CloudTrail.
pci-. dss/v/3.2.1/PCI CloudTrail3.	control de seguridad/ 4CloudTrail.
pci-. dss/v/3.2.1/PCI CloudTrail4.	control de seguridad/ 5CloudTrail.

GeneratorID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
pci-. dss/v/3.2.1/PCI CodeBuild1.	control de seguridad/ 1CodeBuild.
pci-. dss/v/3.2.1/PCI CodeBuild2.	control de seguridad/ 2CodeBuild.
pci-.Config.1 dss/v/3.2.1/PCI	security-control/Config.1
dss/v/3.2.1/PCIpci-C.W.1	control de CloudWatch seguridad/ 1.
pci-D.MS.1 dss/v/3.2.1/PCI	security-control/DMS.1
dss/v/3.2.1/PCIpci-. EC21.	control de seguridad/ 1EC2.
pci-. dss/v/3.2.1/PCI EC22.	control de seguridad/ 2EC2.
pci-. dss/v/3.2.1/PCI EC24.	control de seguridad/ .12 EC2
pci-. dss/v/3.2.1/PCI EC25.	control de seguridad/ .13 EC2
pci-. dss/v/3.2.1/PCI EC26.	control de seguridad/ 6EC2.
pci-. dss/v/3.2.1/PCI ELBv21.	security-control/ELB.1
pci-.ES.1 dss/v/3.2.1/PCI	security-control/ES.2
pci-ES.2 dss/v/3.2.1/PCI	security-control/ES.1
pci-. dss/v/3.2.1/PCI GuardDuty1.	control de seguridad/ 1GuardDuty.
pci-I.AM.1 dss/v/3.2.1/PCI	security-control/IAM.4
dss/v/3.2.1/PCIpci-IAM.2	security-control/IAM.2
dss/v/3.2.1/PCIpci-IAM.3	security-control/IAM.1
dss/v/3.2.1/PCIpci-IAM.4	security-control/IAM.6
dss/v/3.2.1/PCIpci-.IAM.5	security-control/IAM.9
dss/v/3.2.1/PCIpci-.IAM.6	security-control/IAM.19

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
dss/v/3.2.1/PCIpci-.IAM.7	security-control/IAM.8
dss/v/3.2.1/PCIpci-IAM.8	security-control/IAM.10
dss/v/3.2.1/PCIpci-MS.1	security-control/KMS.4
PCI- Lambda.1 dss/v/3.2.1/PCI	security-control/Lambda.1
PCI- Lambda.2 dss/v/3.2.1/PCI	security-control/Lambda.3
dss/v/3.2.1/PCIpci-.Abrir búsqueda.1	security-control/Opensearch.2
dss/v/3.2.1/PCIpci-.Opensearch.2	security-control/Opensearch.1
dss/v/3.2.1/PCIpci-RDS.1	security-control/RDS.1
dss/v/3.2.1/PCIpci-RDS.2	security-control/RDS.2
pci-.Redshift.1 dss/v/3.2.1/PCI	security-control/Redshift.1
dss/v/3.2.1/PCIpci-S3.1	security-control/S3.3
pci-S3.2 dss/v/3.2.1/PCI	security-control/S3.2
pci-S3.3 dss/v/3.2.1/PCI	security-control/S3.7
pci-S.3.5 dss/v/3.2.1/PCI	security-control/S3.5
pci-S3.6 dss/v/3.2.1/PCI	security-control/S3.1
pci-. dss/v/3.2.1/PCI SageMaker1.	control de seguridad/ 1SageMaker.
pci-SSM.1 dss/v/3.2.1/PCI	security-control/SSM.2
dss/v/3.2.1/PCIpci-SSM.2	security-control/SSM.3
dss/v/3.2.1/PCIpci-SSM.3	security-control/SSM.1

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
service-managed-aws-controltower/v/1.0.0/ ACM- 1.	security-control/ACM.1
service-managed-aws-control- tower/v/1.0.0/ APIGateway 1.	control de seguridad/ .1 APIGateway
service-managed-aws-control- 2tower/v/1.0.0/ APIGateway.	control de seguridad/ .2 APIGateway
service-managed-aws-control- 3tower/v/1.0.0/ APIGateway.	control de seguridad/ 3APIGateway.
service-managed-aws-control- 4tower/v/1.0.0/ APIGateway.	control de seguridad/ .4APIGateway.
service-managed-aws-control- 5tower/v/1.0.0/ APIGateway.	control de seguridad/ .5 APIGateway
service-managed-aws-control- 1tower/v/1.0.0/ AutoScaling.	control de seguridad/ .1 AutoScaling
service-managed-aws-control- 2tower/v/1.0.0/ AutoScaling.	control de seguridad/ .2 AutoScaling
service-managed-aws-control- 3tower/v/1.0.0/ AutoScaling.	control de seguridad/ 3AutoScaling.
service-managed-aws-control- 4tower/v/1.0.0/ AutoScaling.	control de seguridad/ .4AutoScaling.
service-managed-aws-control- 5tower/v/1.0.0/ Autoscaling.	security-control/Autoscaling.5
service-managed-aws-control- 6tower/v/1.0.0/ AutoScaling.	control de seguridad/ .6 AutoScaling

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
service-managed-aws-control- 9tower/v/1.0.0/ AutoScaling.	control de seguridad/ .9 AutoScaling
service-managed-aws-control- 1tower/v/1.0.0/ CloudTrail.	control de seguridad/ .1 CloudTrail
service-managed-aws-control- 2tower/v/1.0.0/ CloudTrail.	control de seguridad/ .2 CloudTrail
service-managed-aws-control- 4tower/v/1.0.0/ CloudTrail.	control de seguridad/ .4CloudTrail.
service-managed-aws-control- 5tower/v/1.0.0/ CloudTrail.	control de seguridad/ .5 CloudTrail
service-managed-aws-control- 1tower/v/1.0.0/ CodeBuild.	control de seguridad/ .1 CodeBuild
service-managed-aws-control- 2tower/v/1.0.0/ CodeBuild.	control de seguridad/ .2 CodeBuild
service-managed-aws-control- 4tower/v/1.0.0/ CodeBuild.	control de seguridad/ .4CodeBuild.
service-managed-aws-control- 5tower/v/1.0.0/ CodeBuild.	control de seguridad/ .5 CodeBuild
service-managed-aws-control- 1tower/v/1.0.0/ DMS.	security-control/DMS.1
service-managed-aws-control- tower/v/1.0.0/ DynamoDB 1.	security-control/DynamoDB.1
service-managed-aws-control- tower/v/1.0.0/ DynamoDB 2.	security-control/DynamoDB.2

GeneratorID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
service-managed-aws-control- tower/v/1.0.0/EC 2.1	control de seguridad/ .1 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.2	control de seguridad/ 2EC2.
service-managed-aws-control- tower/v/1.0.0/EC 2.3	control de seguridad/ 3EC2.
service-managed-aws-control- tower/v/1.0.0/EC 2.4	control de seguridad/ 4EC2.
service-managed-aws-control- tower/v/1.0.0/EC 2.6	control de seguridad/ 6EC2.
service-managed-aws-control- tower/v/1.0.0/EC 2.7	control de seguridad/ 7EC2.
service-managed-aws-control- tower/v/1.0.0/EC 2.8	control de seguridad/ 8EC2.
service-managed-aws-control- tower/v/1.0.0/EC 2.9	control de seguridad/ 9EC2.
service-managed-aws-control- tower/v/1.0.0/EC 2.10	control de seguridad/ .10 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.15	control de seguridad/ .15 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.16	control de seguridad/ 1.6 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.17	control de seguridad/ 1.7 EC2

GeneratorID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
service-managed-aws-control- tower/v/1.0.0/EC2.18	control de seguridad/ .18 EC2
service-managed-aws-control- tower/v/1.0.0/EC2.19	control de seguridad/ .19 EC2
service-managed-aws-control- tower/v/1.0.0/EC2.20	control de seguridad/ .20 EC2
service-managed-aws-control- tower/v/1.0.0/EC2.21	control de seguridad/ 2.1 EC2
service-managed-aws-control- tower/v/1.0.0/EC2.22	control de seguridad/ 2.2 EC2
service-managed-aws-control- 1tower/v/1.0.0/ECR.	security-control/ECR.1
service-managed-aws-control- tower/v/1.0.0/ECR 2.	security-control/ECR.2
service-managed-aws-control- tower/v/1.0.0/ECR 3.	security-control/ECR.3
service-managed-aws-control- tower/v/1.0.0/ECS 1.	security-control/ECS.1
service-managed-aws-control- tower/v/1.0.0/ECS 2.	security-control/ECS.2
service-managed-aws-control- tower/v/1.0.0/ECS 3.	security-control/ECS.3
service-managed-aws-control- 4tower/v/1.0.0/ECS.	security-control/ECS.4

GeneratorID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
service-managed-aws-control-5tower/v/1.0.0/ECS.	security-control/ECS.5
service-managed-aws-control-8tower/v/1.0.0/ECS.	security-control/ECS.8
service-managed-aws-control-10tower/v/1.0.0/ECS	security-control/ECS.10
service-managed-aws-control-12tower/v/1.0.0/ECS	security-control/ECS.12
service-managed-aws-control-1tower/v/1.0.0/EFS.	security-control/EFS.1
service-managed-aws-control-2tower/v/1.0.0/EFS 2.	security-control/EFS.2
service-managed-aws-control-3tower/v/1.0.0/EFS 3.	security-control/EFS.3
service-managed-aws-control-4tower/v/1.0.0/EFS.	security-control/EFS.4
service-managed-aws-control-2tower/v/1.0.0/EKS.	security-control/EKS.2
service-managed-aws-control-2tower/v/1.0.0/ELB 2.	security-control/ELB.2
service-managed-aws-control-3tower/v/1.0.0/ELB 3.	security-control/ELB.3
service-managed-aws-control-4tower/v/1.0.0/ELB.	security-control/ELB.4

GeneratorID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
service-managed-aws-control- 5tower/v/1.0.0/ELB.	security-control/ELB.5
service-managed-aws-control- 6tower/v/1.0.0/ELB.	security-control/ELB.6
service-managed-aws-control- 7tower/v/1.0.0/ELB.	security-control/ELB.7
service-managed-aws-control- 8tower/v/1.0.0/ELB.	security-control/ELB.8
service-managed-aws-control- 9tower/v/1.0.0/ELB.	security-control/ELB.9
service-managed-aws-control- .10 tower/v/1.0.0/ELB	security-control/ELB.10
service-managed-aws-control- .12 tower/v/1.0.0/ELB	security-control/ELB.12
service-managed-aws-control- 1.3 tower/v/1.0.0/ELB	security-control/ELB.13
service-managed-aws-control- 1.4 tower/v/1.0.0/ELB	security-control/ELB.14
service-managed-aws-control- 2.1 tower/v/1.0.0/ELBv	control de seguridad/ .1 ELBv2
service-managed-aws-control- tower/v/1.0.0/EMR 1.	security-control/EMR.1
service-managed-aws-control- tower/v/1.0.0/ES 1.	security-control/ES.1

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
service-managed-aws-control- tower/v/1.0.0/ES 2.	security-control/ES.2
service-managed-aws-control- tower/v/1.0.0/ES 3.	security-control/ES.3
service-managed-aws-control- 4tower/v/1.0.0/ ES.	security-control/ES.4
service-managed-aws-control- 5tower/v/1.0.0/ ES.	security-control/ES.5
service-managed-aws-control- 6tower/v/1.0.0/ ES.	security-control/ES.6
service-managed-aws-control- 7tower/v/1.0.0/ ES.	security-control/ES.7
service-managed-aws-control- 8tower/v/1.0.0/ ES.	security-control/ES.8
service-managed-aws-control- 1tower/v/1.0.0/ ElasticBeanstalk.	control de seguridad/ .1 ElasticBeanstalk
service-managed-aws-control- 2tower/v/1.0.0/ ElasticBeanstalk.	control de seguridad/ .2 ElasticBeanstalk
service-managed-aws-control- 1tower/v/1.0.0/ GuardDuty.	control de seguridad/ .1 GuardDuty
service-managed-aws-control- tower/v/1.0.0/ IAM 1.	security-control/IAM.1
service-managed-aws-control- tower/v/1.0.0/ IAM 2.	security-control/IAM.2

GeneratorID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
service-managed-aws-control- tower/v/1.0.0/ IAM 3.	security-control/IAM.3
service-managed-aws-control- 4tower/v/1.0.0/ IAM.	security-control/IAM.4
service-managed-aws-control- 5tower/v/1.0.0/ IAM.	security-control/IAM.5
service-managed-aws-control- 6tower/v/1.0.0/ IAM.	security-control/IAM.6
service-managed-aws-control- 7tower/v/1.0.0/ IAM.	security-control/IAM.7
service-managed-aws-control- 8tower/v/1.0.0/ IAM.	security-control/IAM.8
service-managed-aws-control- 2.1 tower/v/1 .0.0/IAM	security-control/IAM.21
service-managed-aws-control- 1tower/v/1.0.0/ Kinesis.	security-control/Kinesis.1
service-managed-aws-control- tower/v/1.0.0/ KMS 1.	security-control/KMS.1
service-managed-aws-control- tower/v/1.0.0/ KMS 2.	security-control/KMS.2
service-managed-aws-control- tower/v/1.0.0/ KMS 3.	security-control/KMS.3
service-managed-aws-control- tower/v/1.0.0/ Lambda 1.	security-control/Lambda.1

GeneratorID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
service-managed-aws-control- tower/v/1.0.0/ Lambda 2.	security-control/Lambda.2
service-managed-aws-control- 5tower/v/1.0.0/ Lambda.	security-control/Lambda.5
service-managed-aws-control- 3tower/v/1.0.0/ NetworkFirewall.	control de seguridad/ 3NetworkFirewall.
service-managed-aws-control- 4tower/v/1.0.0/ NetworkFirewall.	control de seguridad/ .4NetworkFirewall.
service-managed-aws-control- 5tower/v/1.0.0/ NetworkFirewall.	control de seguridad/ .5 NetworkFirewall
service-managed-aws-control- 6tower/v/1.0.0/ NetworkFirewall.	control de seguridad/ .6 NetworkFirewall
service-managed-aws-control- 1tower/v/1.0.0/ Opensearch.	security-control/Opensearch.1
service-managed-aws-control- tower/v/1.0.0/ Opensearch 2.	security-control/Opensearch.2
service-managed-aws-control- tower/v/1.0.0/ Opensearch 3.	security-control/Opensearch.3
service-managed-aws-control- 4tower/v/1.0.0/ Opensearch.	security-control/Opensearch.4
service-managed-aws-control- 5tower/v/1.0.0/ Opensearch.	security-control/Opensearch.5
service-managed-aws-control- 6tower/v/1.0.0/ Opensearch.	security-control/Opensearch.6

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
service-managed-aws-control- 7tower/v/1.0.0/Opensearch.	security-control/Opensearch.7
service-managed-aws-control- 8tower/v/1.0.0/Opensearch.	security-control/Opensearch.8
service-managed-aws-control- 1tower/v/1.0.0/RDS.	security-control/RDS.1
service-managed-aws-control- tower/v/1.0.0/RDS 2.	security-control/RDS.2
service-managed-aws-control- tower/v/1.0.0/RDS 3.	security-control/RDS.3
service-managed-aws-control- 4tower/v/1.0.0/RDS.	security-control/RDS.4
service-managed-aws-control- 5tower/v/1.0.0/RDS.	security-control/RDS.5
service-managed-aws-control- 6tower/v/1.0.0/RDS.	security-control/RDS.6
service-managed-aws-control- 8tower/v/1.0.0/RDS.	security-control/RDS.8
service-managed-aws-control- 9tower/v/1.0.0/RDS.	security-control/RDS.9
service-managed-aws-control- .10 tower/v/1.0.0/RDS	security-control/RDS.10
service-managed-aws-control- .11 tower/v/1.0.0/RDS	security-control/RDS.11

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
service-managed-aws-control- 1.3 tower/v/1 .0.0/RDS	security-control/RDS.13
service-managed-aws-control- 1.7 tower/v/1 .0.0/RDS	security-control/RDS.17
service-managed-aws-control- .18 tower/v/1 .0.0/RDS	security-control/RDS.18
service-managed-aws-control- 1.9 tower/v/1 .0.0/RDS	security-control/RDS.19
service-managed-aws-control- 2.0 tower/v/1 .0.0/RDS	security-control/RDS.20
service-managed-aws-control- 2.1 tower/v/1 .0.0/RDS	security-control/RDS.21
service-managed-aws-control- .22 tower/v/1 .0.0/RDS	security-control/RDS.22
service-managed-aws-control- 2.3 tower/v/1 .0.0/RDS	security-control/RDS.23
service-managed-aws-control- .25 tower/v/1 .0.0/RDS	security-control/RDS.25
service-managed-aws-control- 1tower/v/1.0.0/ Redshift.	security-control/Redshift.1
service-managed-aws-control- tower/v/1.0.0/ Redshift 2.	security-control/Redshift.2
service-managed-aws-control- 4tower/v/1.0.0/ Redshift.	security-control/Redshift.4

GeneratorID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
service-managed-aws-control- 6tower/v/1.0.0/Redshift.	security-control/Redshift.6
service-managed-aws-control- 7tower/v/1.0.0/Redshift.	security-control/Redshift.7
service-managed-aws-control- 8tower/v/1.0.0/Redshift.	security-control/Redshift.8
service-managed-aws-control- 9tower/v/1.0.0/Redshift.	security-control/Redshift.9
service-managed-aws-control- 3.1 tower/v/1.0.0/S	security-control/S3.1
service-managed-aws-control- tower/v/1.0.0/S 3.2	security-control/S3.2
service-managed-aws-control- tower/v/1.0.0/S 3.3	security-control/S3.3
service-managed-aws-control- tower/v/1.0.0/S 3.5	security-control/S3.5
service-managed-aws-control- tower/v/1.0.0/S 3.6	security-control/S3.6
service-managed-aws-control- tower/v/1.0.0/S 3.8	security-control/S3.8
service-managed-aws-control- tower/v/1.0.0/S 3.9	security-control/S3.9
service-managed-aws-control- tower/v/1.0.0/S 3.12	security-control/S3.12

GeneratorID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
service-managed-aws-control- 3,13 tower/v/1.0.0/S	security-control/S3.13
service-managed-aws-control- 1tower/v/1.0.0/SageMaker.	control de seguridad/ .1 SageMaker
service-managed-aws-control- tower/v/1.0.0/SecretsManager 1.	control de seguridad/ .1 SecretsManager
service-managed-aws-control- 2tower/v/1.0.0/SecretsManager.	control de seguridad/ .2 SecretsManager
service-managed-aws-control- 3tower/v/1.0.0/SecretsManager.	control de seguridad/ 3SecretsManager.
service-managed-aws-control- 4tower/v/1.0.0/SecretsManager.	control de seguridad/ .4SecretsManager.
service-managed-aws-control- 1tower/v/1.0.0/SQS.	security-control/SQS.1
service-managed-aws-control- tower/v/1.0.0/SSM 1.	security-control/SSM.1
service-managed-aws-control- tower/v/1.0.0/SSM 2.	security-control/SSM.2
service-managed-aws-control- tower/v/1.0.0/SSM 3.	security-control/SSM.3
service-managed-aws-control- 4tower/v/1.0.0/SSM.	security-control/SSM.4
service-managed-aws-control- 2tower/v/1.0.0/WAF.	security-control/WAF.2

GeneratID antes de permitir la consolidación de los resultados de control	GeneratorID después de habilitar los hallazgos de control consolidados
service-managed-aws-control- tower/v/1.0.0/WAF.3.	security-control/WAF.3
service-managed-aws-control- 4tower/v/1.0.0/WAF.	security-control/WAF.4

Cómo afecta la consolidación al control IDs y a los títulos

La vista de los controles consolidados y los resultados de los controles consolidados estandarizan el control IDs y los títulos en todos los estándares. Los términos Identificador de control de seguridad y título de control de seguridad se refieren a estos valores independientes de los estándares.

La consola CSPM de Security Hub muestra títulos de control de seguridad IDs y control de seguridad independientes de los estándares, independientemente de si Consolidated Control Findings está habilitado o desactivado para su cuenta. Sin embargo, las conclusiones del CSPM de Security Hub contienen títulos de control específicos de la norma, para PCI DSS y CIS v1.2.0, si las conclusiones de control consolidadas están deshabilitadas para su cuenta. Además, las conclusiones del CSPM de Security Hub contienen el ID de control y el ID de control de seguridad específicos del estándar. Para ver ejemplos de cómo la consolidación afecta a los resultados de control, consulte [Muestras de los resultados de los controles](#)

En el caso de los controles que forman parte del [estándar de AWS Control Tower gestión de servicios](#), el prefijo CT. se elimina del identificador y el título del control en las conclusiones cuando las conclusiones de control consolidadas están habilitadas.

Para deshabilitar un control de seguridad en Security Hub CSPM, debe deshabilitar todos los controles estándar que correspondan al control de seguridad. En la siguiente tabla se muestra la asignación del control de seguridad IDs y los títulos a los controles y títulos específicos del estándar. IDs IDs y los títulos de los controles que pertenecen al estándar AWS Foundational Security Best Practices (FSBP) ya son independientes del estándar. Para asignar los controles a los requisitos de Center for Internet Security (CIS) v3.0.0 (CIS), consulte [Asignación de los controles a los requisitos del CIS en cada versión](#). Para ejecutar sus propios scripts en esta tabla, puede [descargarlos](#) como un archivo.csv.

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.2.0	1.1 Evitar el uso del usuario raíz	[CloudWatch.1] Debe existir un filtro de métricas de registro y una alarma para el uso del usuario «raíz»
CIS v1.2.0	1.10 Asegurar que la política de contraseñas de IAM impide la reutilización de contraseñas	[IAM.16] Asegurar que la política de contraseñas de IAM impida la reutilización de contraseñas
CIS v1.2.0	1.11 Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos	[IAM.17] Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos
CIS v1.2.0	1.12 Asegurar que no existe una clave de acceso del usuario raíz	[IAM.4] La clave de acceso del usuario raíz de IAM no debería existir
CIS v1.2.0	1.13 Asegurar que la MFA está activada para el usuario raíz	[IAM.9] La MFA debe estar habilitada para el usuario raíz
CIS v1.2.0	1.14 Asegurar que la MFA está activada para el usuario raíz	[PCI.IAM.6] La MFA de hardware debe estar habilitada para el usuario raíz
CIS v1.2.0	1.16 Asegurar que las políticas de IAM solo están asociadas a grupos o roles	[IAM.2] Los usuarios de IAM no deben tener políticas de IAM asociadas
CIS v1.2.0	1.2 Asegurar que la autenticación multifactor (MFA) está habilitada para todos los usuarios de IAM que tienen una contraseña de la consola	[IAM.5] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola
CIS v1.2.0	1.20 Asegurar que se ha creado un rol de soporte para administrar incidentes con Soporte	[IAM.18] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.2.0	1.22 Asegurar que no se crean políticas de IAM que permiten privilegios administrativos completos “*. *”	[IAM.1] Las políticas de IAM no deben permitir privilegios administrativos completos “*”
CIS v1.2.0	1.3 Asegurar que se deshabilitan las credenciales no usadas durante 90 días o más	[IAM.8] Deben eliminarse las credenciales de usuario de IAM no utilizadas
CIS v1.2.0	1.4 Asegurar que las claves de acceso se rotan cada 90 días o menos	[IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
CIS v1.2.0	1.5 Asegurar que la política de contraseñas de IAM requiere al menos una letra mayúscula	[IAM.11] Asegurar que la política de contraseñas de IAM requiera al menos una letra mayúscula
CIS v1.2.0	1.6 Asegurar que la política de contraseñas de IAM requiere al menos una letra minúscula	[IAM.12] Asegurar que la política de contraseñas de IAM requiera al menos una letra minúscula
CIS v1.2.0	1.7 Asegurar que la política de contraseñas de IAM requiere al menos un símbolo	[IAM.13] Asegurar que la política de contraseñas de IAM requiera al menos un símbolo
CIS v1.2.0	1.8 Asegurar que la política de contraseñas de IAM requiere al menos un número	[IAM.14] Asegurar que la política de contraseñas de IAM requiera al menos un número
CIS v1.2.0	1.9 Asegurar que la política de contraseñas de IAM requiere una longitud mínima de 14 o más	[IAM.15] Asegurar que la política de contraseñas de IAM requiera una longitud mínima de 14 o más

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.2.0	2.1 Asegúrese de que CloudTrail esté activado en todas las regiones	[CloudTrail.1] CloudTrail debe habilitarse y configurarse con al menos un registro de seguimiento para varias regiones que incluya eventos de administración de lectura y escritura
CIS v1.2.0	2.2 Asegúrese de que la validación del archivo de CloudTrail registro esté habilitada	[CloudTrail.4] La validación de archivo de CloudTrail registro debe estar habilitada
CIS v1.2.0	2.3 Asegúrese de que el depósito de S3 utilizado para almacenar CloudTrail los registros no sea de acceso público	[CloudTrail.6] Asegurar que los CloudTrail registros del bucket de S3 no son de acceso público
CIS v1.2.0	2.4 Asegúrese de que los CloudTrail senderos estén integrados con CloudWatch los registros	[CloudTrail.5] CloudTrail Los senderos deben estar integrados con Amazon Logs CloudWatch
CIS v1.2.0	2.5 Asegúrese de que AWS Config esté activado	[Config.1] AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos
CIS v1.2.0	2.6 Asegúrese de que el registro de acceso al bucket de S3 esté habilitado o en el bucket de CloudTrail S3	[CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el bucket de CloudTrail S3
CIS v1.2.0	2.7 Asegúrese de que CloudTrail los registros estén cifrados en reposo mediante KMS CMKs	[CloudTrail.2] CloudTrail debe tener habilitado el cifrado en reposo

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.2.0	2.8 Asegúrese de que la rotación para los clientes creados CMKs esté habilitada	La rotación de AWS KMS teclas [KMS.4] debe estar habilitada
CIS v1.2.0	2.9 Asegúrese de que el registro de flujo de VPC esté habilitado en todas VPCs	[EC2.6] El registro de flujos de VPC debe estar habilitado en todos VPCs
CIS v1.2.0	3.1 Asegurar que haya un filtro de métricas de registro y alarma para las llamadas no autorizadas a la API	[CloudWatch.2] Asegurar que haya un filtro de métricas de registro y alarma para las llamadas a la API no autorizadas
CIS v1.2.0	3.10 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de grupos de seguridad	[CloudWatch.10] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de grupos de seguridad
CIS v1.2.0	3.11 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios en las listas de control de acceso a la red (NACL)	[CloudWatch.11] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios en las listas de control de acceso a la red (NACL)
CIS v1.2.0	3.12 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a las gateways de la red	[CloudWatch.12] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a las puertas de enlace de la red
CIS v1.2.0	3.13 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a la tabla de enrutamiento	[CloudWatch.13] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a la tabla de enrutamiento

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.2.0	3.14 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de VPC	[CloudWatch.14] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de VPC
CIS v1.2.0	3.2 Asegurar que haya un filtro de métricas de registro y alarma de registro para el inicio de sesión en la Consola de administración sin MFA	[CloudWatch.3] Asegurar que haya un filtro de métricas de registro y alarma de registro para el inicio de sesión en la Consola de administración sin MFA
CIS v1.2.0	3.3 Asegurar que haya un filtro de métricas de registro y alarma de registro para el uso del usuario raíz	[CloudWatch.1] Debe existir un filtro de métricas de registro y una alarma para el uso del usuario «raíz»
CIS v1.2.0	3.4 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de IAM	[CloudWatch.4] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de IAM
CIS v1.2.0	3.5 Asegúrese de que existan un registro métrico, un filtro y una alarma para los cambios CloudTrail de configuración	[CloudWatch.5] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de CloudTrail configuración de
CIS v1.2.0	3.6 Asegúrese de que existan un filtro de métrica de registro y una alarma para detectar errores AWS Management Console de autenticación	[CloudWatch.6] Asegurar que haya un filtro de métricas de registro y alarma de registro para los errores de AWS Management Console autenticación

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.2.0	3.7 Asegúrese de que existan un filtro de métricas de registro y una alarma para deshabilitar o eliminar de forma programada los datos creados por el cliente CMKs	[CloudWatch.7] Asegurar que haya un filtro de métricas de registro y alarma de registro para la deshabilitación o eliminación programada de claves administradas por el cliente
CIS v1.2.0	3.8 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de bucket de S3	[CloudWatch.8] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de bucket de S3
CIS v1.2.0	3.9 Asegúrese de que existan un filtro de registro métrico y una alarma para los cambios AWS Config de configuración	[CloudWatch.9] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de AWS Config configuración de
CIS v1.2.0	4.1 Asegurar que ningún grupo de seguridad permita la entrada desde 0.0.0.0/0 al puerto 22	[EC2.13] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0.0.0.0/0 o: :/0 al puerto 22
CIS v1.2.0	4.2 Asegurar que ningún grupo de seguridad permita la entrada desde 0.0.0.0/0 al puerto 3389	[EC2.14] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0.0.0.0/0 o: :/0 al puerto 3389
CIS v1.2.0	4.3 Asegurar que el grupo de seguridad predeterminado de cada VPC limita todo el tráfico	[EC2.22] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente
CIS v1.4.0	1.10 Asegurar que la autenticación multifactor (MFA) está habilitada para todos los usuarios de IAM que tienen una contraseña de la consola	[IAM.5] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.4.0	1.14 Asegurar que las claves de acceso se rotan cada 90 días o menos	[IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos
CIS v1.4.0	1.16 Asegurar que no se adjunten políticas de IAM que permitan privilegios administrativos completos “*.*”	[IAM.1] Las políticas de IAM no deben permitir privilegios administrativos completos “*”
CIS v1.4.0	1.17 Asegurar que se ha creado un rol de soporte para administrar incidentes con Soporte	[IAM.18] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support
CIS v1.4.0	1.4 Asegurar que no existe una clave de acceso del usuario raíz	[IAM.4] La clave de acceso del usuario raíz de IAM no debería existir
CIS v1.4.0	1.5 Asegurar que la MFA esté activada para el usuario raíz	[IAM.9] La MFA debe estar habilitada para el usuario raíz
CIS v1.4.0	1.6 Asegurar que la MFA basada en hardware está activada para el usuario raíz	[PCI.IAM.6] La MFA de hardware debe estar habilitada para el usuario raíz
CIS v1.4.0	1.7 Elimine el uso del usuario raíz para las tareas administrativas y diarias	[CloudWatch.1] Debe existir un filtro de métricas de registro y una alarma para el uso del usuario «raíz»
CIS v1.4.0	1.8 Asegurar que la política de contraseñas de IAM requiere una longitud mínima de 14 o más	[IAM.15] Asegurar que la política de contraseñas de IAM requiera una longitud mínima de 14 o más
CIS v1.4.0	1.9 Asegurar que la política de contraseñas de IAM impide la reutilización de contraseñas	[IAM.16] Asegurar que la política de contraseñas de IAM impida la reutilización de contraseñas

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.4.0	2.1.2 Asegúrese de que la política de buckets de S3 esté configurada para denegar las solicitudes HTTP	[S3.5] En las solicitudes de los buckets de uso general de S3, se debe pedir el uso de SSL
CIS v1.4.0	2.1.5.1 La configuración de S3 Block Public Access debe estar habilitada	[S3.1] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público
CIS v1.4.0	2.1.5.2 La configuración de acceso público al bloque S3 debe estar habilitada en el nivel de bucket	[S3.8] Los buckets de uso general de S3 deben bloquear el acceso público
CIS v1.4.0	2.2.1 Asegúrese de que el cifrado de volúmenes de EBS esté activado	[EC2.7] El cifrado predeterminado de EBS debe estar activado
CIS v1.4.0	2.3.1 Asegúrese de que el cifrado esté habilitado para las instancias RDS	[RDS.3] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo
CIS v1.4.0	3.1 Asegúrese de que CloudTrail esté activado en todas las regiones	[CloudTrail.1] CloudTrail debe habilitarse y configurarse con al menos un registro de seguimiento para varias regiones que incluya eventos de administración de lectura y escritura
CIS v1.4.0	3.2 Asegúrese de que la validación del archivo de CloudTrail registro esté habilitada	[CloudTrail.4] La validación de archivo de CloudTrail registro debe estar habilitada
CIS v1.4.0	3.4 Asegúrese de que los CloudTrail senderos estén integrados con CloudWatch los registros	[CloudTrail.5] CloudTrail Los senderos deben estar integrados con Amazon Logs CloudWatch

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.4.0	3.5 Asegúrese de que AWS Config esté habilitado en todas las regiones	[Config.1] AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos
CIS v1.4.0	3.6 Asegúrese de que el registro de acceso al bucket de S3 esté habilitado o en el bucket de CloudTrail S3	[CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el bucket de CloudTrail S3
CIS v1.4.0	3.7 Asegúrese de que CloudTrail los registros estén cifrados en reposo mediante KMS CMKs	[CloudTrail.2] CloudTrail debe tener habilitado el cifrado en reposo
CIS v1.4.0	3.8 Asegúrese de que la rotación para los clientes creados CMKs esté habilitada	La rotación de AWS KMS teclas [KMS.4] debe estar habilitada
CIS v1.4.0	3.9 Asegúrese de que el registro de flujo de VPC esté habilitado en todas VPCs	[EC2.6] El registro de flujos de VPC debe estar habilitado en todos VPCs
CIS v1.4.0	4.4 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de IAM	[CloudWatch.4] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de IAM
CIS v1.4.0	4.5 Asegúrese de que existan un registro métrico, un filtro y una alarma para los cambios CloudTrail de configuración	[CloudWatch.5] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de CloudTrail configuración de

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.4.0	4.6 Asegúrese de que existan un filtro de métrica de registro y una alarma para detectar errores AWS Management Console de autenticación	[CloudWatch.6] Asegurar que haya un filtro de métricas de registro y alarma de registro para los errores de AWS Management Console autenticación
CIS v1.4.0	4.7 Asegúrese de que existan un filtro de métricas de registro y una alarma para deshabilitar o eliminar de forma programada lo creado por el cliente CMKs	[CloudWatch.7] Asegurar que haya un filtro de métricas de registro y alarma de registro para la deshabilitación o eliminación programada de claves administradas por el cliente
CIS v1.4.0	4.8 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de bucket de S3	[CloudWatch.8] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de política de bucket de S3
CIS v1.4.0	4.9 Asegúrese de que existan un filtro de registro métrico y una alarma para los cambios AWS Config de configuración	[CloudWatch.9] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de AWS Config configuración de
CIS v1.4.0	4.10 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de grupos de seguridad	[CloudWatch.10] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de grupos de seguridad
CIS v1.4.0	4.11 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios en las listas de control de acceso a la red (NACL)	[CloudWatch.11] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios en las listas de control de acceso a la red (NACL)

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
CIS v1.4.0	4.12 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a las puertas de enlace de la red	[CloudWatch.12] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a las puertas de enlace de la red
CIS v1.4.0	4.13 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios ala tabla de enrutamiento	[CloudWatch.13] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios ala tabla de enrutamiento
CIS v1.4.0	4.14 Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de VPC	[CloudWatch.14] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de VPC
CIS v1.4.0	5.1 Asegúrese de que ninguna red ACLs permita el ingreso desde el 0.0.0.0/0 a los puertos de administración remota del servidor	[EC2.21] La red no ACLs debe permitir la entrada desde 0.0.0/0 al puerto 22 o al puerto 3389
CIS v1.4.0	5.3 Asegurar que el grupo de seguridad predeterminado de cada VPC limita todo el tráfico	[EC22] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente
PCI DSS v3.2.1	PCI. AutoScaling.1 Los grupos de escalado automático asociados a un balanceador de cargas deben usar las comprobaciones de estado del balanceador de cargas	[AutoScaling.1] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar las comprobaciones de estado del ELB
PCI DSS v3.2.1	PCI. CloudTrail.1 CloudTrail Los registros deben cifrarse en reposo mediante AWS KMS CMKs	[CloudTrail.2] CloudTrail debe tener habilitado el cifrado en reposo

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
PCI DSS v3.2.1	PCI. CloudTrail.2 CloudTrail debería estar activado	[CloudTrail.3] Al menos un CloudTrail registro de seguimiento debe habilitarse
PCI DSS v3.2.1	PCI. CloudTrail.3 La validación del archivo de CloudTrail registro debe estar habilitada	[CloudTrail.4] La validación de archivo de CloudTrail registro debe estar habilitada
PCI DSS v3.2.1	PCI. CloudTrail.4 Las CloudTrail rutas deberían estar integradas con Amazon Logs CloudWatch	[CloudTrail.5] CloudTrail Los senderos deben estar integrados con Amazon Logs CloudWatch
PCI DSS v3.2.1	PCI. CodeBuild.1 CodeBuild GitHub o el repositorio fuente de Bitbucket debe usar URLs OAuth	[CodeBuild.1] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales
PCI DSS v3.2.1	PCI. CodeBuild.2 Las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro	[CodeBuild.2] Las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro
PCI DSS v3.2.1	PCI.config.1 debe estar activado AWS Config	[Config.1] AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos
PCI DSS v3.2.1	PCI.CW.1 Debe existir un filtro de métrica de registro y una alarma para el uso del usuario "raíz"	[CloudWatch.1] Debe existir un filtro de métricas de registro y una alarma para el uso del usuario «raíz»
PCI DSS v3.2.1	Las instancias de replicación del Servicio de migración de bases de datos PCI.DMS.1 no deben ser públicas	[DMS.1] Las instancias de replicación de Database Migration Service no deben ser públicas

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
PCI DSS v3.2.1	PCI. EC2.1 Las instantáneas de EBS no deberían poder restaurarse públicamente	[EC2.1] Las instantáneas de Amazon EBS no se deben poder restaurar públicamente
PCI DSS v3.2.1	PCI. EC2.2 El grupo de seguridad predeterminado de VPC debe prohibir el tráfico entrante y saliente	[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante ni saliente
PCI DSS v3.2.1	PCI. EC2.4. Los que no estén usados EC2 EIPs deben ser removidos	[EC2.12] Amazon no utilizado EC2 EIPs debería retirarse
PCI DSS v3.2.1	FOTO. EC2.5 Los grupos de seguridad no deberían permitir la entrada del 0.0.0.0/0 al puerto 22	[EC2.13] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0.0.0.0/0 o: :/0 al puerto 22
PCI DSS v3.2.1	PCI. EC2.6 El registro de flujo de VPC debe estar habilitado en todas VPCs	[EC2.6] El registro de flujos de VPC debe estar habilitado en todos VPCs
PCI DSS v3.2.1	PCI. ELBv2.1 Application Load Balancer debe configurarse para redirigir todas las solicitudes HTTP a HTTPS	[ELB.1] El equilibrador de carga de aplicación debe configurarse para redirigir todas las solicitudes HTTP a HTTPS
PCI DSS v3.2.1	PCI.ES.1 Los dominios de Elasticsearch deberían estar en una VPC	[ES.2] Los dominios de Elasticsearch no deben ser de acceso público
PCI DSS v3.2.1	PCI.ES.2 Los dominios de Elasticsearch deben tener habilitado el cifrado en reposo	[ES.1] Los dominios de Elasticsearch deben tener habilitado el cifrado en reposo
PCI DSS v3.2.1	PCI. GuardDuty.1 GuardDuty debe estar activado	[GuardDuty.1] GuardDuty debería estar activado
PCI DSS v3.2.1	PCI.IAM.1 La clave de acceso de usuario raíz de IAM no debe existir	[IAM.4] La clave de acceso del usuario raíz de IAM no debería existir

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
PCI DSS v3.2.1	PCI.IAM.2 Los usuarios de IAM no deben tener políticas de IAM asociadas	[IAM.2] Los usuarios de IAM no deben tener políticas de IAM asociadas
PCI DSS v3.2.1	PCI.IAM.3 Las políticas de IAM no deben permitir privilegios administrativos completos «*»	[IAM.1] Las políticas de IAM no deben permitir privilegios administrativos completos «*»
PCI DSS v3.2.1	PCI.IAM.4 La MFA de hardware debe estar habilitada para el usuario raíz	[PCI.IAM.6] La MFA de hardware debe estar habilitada para el usuario raíz
PCI DSS v3.2.1	PCI.IAM.5 La MFA virtual debe estar habilitada para el usuario raíz	[IAM.9] La MFA debe estar habilitada para el usuario raíz
PCI DSS v3.2.1	PCI.IAM.6 MFA se debe habilitar para todos los usuarios de IAM	[IAM.19] MFA se debe habilitar para todos los usuarios de IAM
PCI DSS v3.2.1	PCI.IAM.7 Las credenciales de usuario de IAM deben deshabilitarse si no se utilizan en un número de días predefinido	[IAM.8] Deben eliminarse las credenciales de usuario de IAM no utilizadas
PCI DSS v3.2.1	PCI.IAM.8 Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras	[IAM.10] Las políticas de contraseñas de usuarios de IAM deben tener configuraciones seguras
PCI DSS v3.2.1	PCI.KMS.1 La rotación de la clave maestra del cliente (CMK) debe estar habilitada	La rotación de AWS KMS teclas [KMS.4] debe estar habilitada
PCI DSS v3.2.1	PCI.lambda.1 Las funciones de Lambda deberían prohibir el acceso público	[Lambda.1] Las políticas de función de Lambda deberían prohibir el acceso público

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
PCI DSS v3.2.1	PCI.lambda.2 Las funciones de Lambda deben estar en una VPC	[Lambda.3] Las funciones de Lambda deben estar en una VPC
PCI DSS v3.2.1	Los OpenSearch dominios PCI.openSearch.1 deben estar en una VPC	Los OpenSearch dominios [Opensearch.2] no deben ser de acceso público
PCI DSS v3.2.1	PCI.Opensearch.2 Las instantáneas de EBS no se deben poder restaurar públicamente	Los OpenSearch dominios [Opensearch.1] deben tener activado el cifrado en reposo
PCI DSS v3.2.1	PCI.RDS.1 Las instantáneas de RDS deben ser privadas	[RDS.1] La instantánea de RDS debe ser privada
PCI DSS v3.2.1	PCI.RDS.2 Las instancias de base de datos de RDS deberían prohibir el acceso público	[RDS.2] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible
PCI DSS v3.2.1	PCI.Redshift.1 Los clústeres de Amazon Redshift deberían prohibir el acceso público	[Redshift.1] Los clústeres de Amazon Redshift deberían prohibir el acceso público
PCI DSS v3.2.1	PCI.S3.1 Los buckets de S3 deberían prohibir el acceso de escritura pública	[S3.3] Los buckets de uso general de S3 deben bloquear el acceso público de escritura
PCI DSS v3.2.1	PCI.S3.2 Los buckets de S3 deberían prohibir el acceso público de lectura	[S3.2] Los buckets de uso general de S3 deben bloquear el acceso público de lectura
PCI DSS v3.2.1	PCI.S3.3 Los buckets de S3 deben tener habilitada la replicación entre regiones	[S3.7] Los buckets de uso general de S3 deben usar la replicación entre regiones

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
PCI DSS v3.2.1	Los buckets PCI.S3.5 S3 deberían requerir solicitudes para usar Secure Socket Layer	[S3.5] En las solicitudes de los buckets de uso general de S3, se debe pedir el uso de SSL
PCI DSS v3.2.1	PCI.S3.6 La configuración de S3 Block Public Access debe estar habilitada	[S3.1] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público
PCI DSS v3.2.1	PCI. SageMaker.1 Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet	[SageMaker.1] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet
PCI DSS v3.2.1	Las instancias PCI.SSM.1 EC2 administradas por Systems Manager deben tener el estado de conformidad con los parches de CONFORMIDAD CON LOS PARCHES tras la instalación de un parche	[SSM.2] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de parche de COMPLIANT después de la instalación de un parche
PCI DSS v3.2.1	Las instancias PCI.SSM.2 EC2 administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT	[SSM.3] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT
PCI DSS v3.2.1	Las instancias PCI.SSM.3 deben administrarse mediante EC2 AWS Systems Manager	[SSM.1] EC2 Las instancias de Amazon deben administrarse mediante AWS Systems Manager

Actualización de los flujos de trabajo para la consolidación

Si sus flujos de trabajo no se basan en el formato específico de ningún campo de los resultados de control, no es necesario realizar ninguna acción.

Si sus flujos de trabajo se basan en el formato específico de uno o más campos en las conclusiones de los controles, como se indica en las tablas anteriores, debe actualizar los flujos de trabajo. Por ejemplo, si ha creado una EventBridge regla de Amazon que desencadena una acción para un ID de control específico, como invocar una AWS Lambda función si el ID de control es igual a CIS 2.7, actualice la regla para que utilice CloudTrail .2, que es el valor del `Compliance.SecurityControlId` campo de ese control.

Si ha creado [estadísticas personalizadas](#) que utilizan alguno de los campos o valores que han cambiado, actualice esas estadísticas para utilizar los nuevos campos o valores.

Atributos de nivel superior necesarios del ASFF

Los siguientes atributos de nivel superior en el formato de búsqueda de AWS seguridad (ASFF) son necesarios para todos los hallazgos en Security Hub CSPM. Para obtener más información sobre estos atributos, consulte [AwsSecurityFinding](#) la Referencia de la API de AWS Security Hub.

AwsAccountId

El Cuenta de AWS ID al que se aplica el hallazgo.

Ejemplo

```
"AwsAccountId": "111111111111"
```

CreatedAt

Indica cuándo se creó el posible problema de seguridad o evento capturado por un hallazgo.

Ejemplo

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

Descripción

Una descripción del hallazgo. Este campo puede ser texto reutilizable no específico o información específica de la instancia del hallazgo.

Para los hallazgos de control que genera Security Hub CSPM, este campo proporciona una descripción del control.

Este campo no hace referencia a un estándar si activa los [resultados de control consolidados](#).

Ejemplo

```
"Description": "This AWS control checks whether AWS Config is enabled in the current account and Region."
```

GeneratorId

El identificador para el componente específico de la solución (unidad de lógica discreta) que generó un hallazgo.

Para los hallazgos de control que genera el CSPM de Security Hub, este campo no hace referencia a un estándar si se activan los hallazgos de [control consolidados](#).

Ejemplo

```
"GeneratorId": "security-control/Config.1"
```

Id

El identificador específico del producto para un hallazgo. Para los hallazgos de control que genera Security Hub CSPM, este campo proporciona el nombre de recurso de Amazon (ARN) del hallazgo.

Este campo no hace referencia a un estándar si activa los [resultados de control consolidados](#).

Ejemplo

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/ab6d6a26-a156-48f0-9403-115983e5a956"
```

ProductArn

El nombre de recurso de Amazon (ARN) generado por Security Hub CSPM, que identifica de forma exclusiva un producto de terceros, encuentra un producto una vez registrado el producto en Security Hub CSPM.

El formato de este campo es `arn:partition:securityhub:region:account-id:product/company-id/product-id`.

- Para Servicios de AWS que estén integrados con Security Hub CSPM, `company-id` debe ser `aws` y `product-id` debe ser el nombre del servicio AWS público. Como AWS los productos y servicios no están asociados a una cuenta, la `account-id` sección del ARN está vacía. Servicios

de AWS los productos que aún no estén integrados con Security Hub CSPM se consideran productos de terceros.

- En el caso de productos públicos, el `company-id` y el `product-id` deben ser los valores de ID especificados en el momento del registro.
- En el caso de productos privados, el `company-id` debe ser el ID de la cuenta. El `product-id` debe ser la palabra reservada de forma predeterminada o el ID que se especificó en el momento del registro.

Ejemplo

```
// Private ARN
  "ProductArn": "arn:aws:securityhub:us-east-1:111111111111:product/111111111111/default"

// Public ARN
  "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty"
  "ProductArn": "arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-pro"
```

Recursos

La `Resources` matriz de objetos proporciona un conjunto de tipos de datos de recursos que describen AWS los recursos a los que se refiere el hallazgo. Para obtener más información sobre los campos que puede contener un `Resources` objeto, incluidos los campos obligatorios, consulte [Resource](#) la Referencia de la API de AWS Security Hub. Para ver ejemplos de `Resources` objetos específicos Servicios de AWS, consulte [Objeto Resources del ASFF](#).

Ejemplo

```
"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/SampleApp/1234567890abcdef0",
    "ApplicationName": "SampleApp",
    "DataClassification": {
      "DetailedResultsLocation": "Path_to_Folder_or_File",
      "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
```

```

    "Status": {
      "Code": "COMPLETE",
      "Reason": "Unsupportedfield"
    },
    "SensitiveData": [
      {
        "Category": "PERSONAL_INFORMATION",
        "Detections": [
          {
            "Count": 34,
            "Type": "GE_PERSONAL_ID",
            "Occurrences": {
              "LineRanges": [
                {
                  "Start": 1,
                  "End": 10,
                  "StartColumn": 20
                }
              ],
              "Pages": [],
              "Records": [],
              "Cells": []
            }
          },
          {
            "Count": 59,
            "Type": "EMAIL_ADDRESS",
            "Occurrences": {
              "Pages": [
                {
                  "PageNumber": 1,
                  "OffsetRange": {
                    "Start": 1,
                    "End": 100,
                    "StartColumn": 10
                  },
                  "LineRange": {
                    "Start": 1,
                    "End": 100,
                    "StartColumn": 10
                  }
                }
              ]
            }
          }
        ]
      }
    ]
  }

```

```

    },
    {
      "Count": 2229,
      "Type": "URL",
      "Occurrences": {
        "LineRanges": [
          {
            "Start": 1,
            "End": 13
          }
        ]
      }
    },
    {
      "Count": 13826,
      "Type": "NameDetection",
      "Occurrences": {
        "Records": [
          {
            "RecordIndex": 1,
            "JsonPath": "$.ssn.value"
          }
        ]
      }
    },
    {
      "Count": 32,
      "Type": "AddressDetection"
    }
  ],
  "TotalCount": 32
},
{
  "CustomDataIdentifiers": {
    "Detections": [
      {
        "Arn": "1712be25e7c7f53c731fe464f1c869b8",
        "Name": "1712be25e7c7f53c731fe464f1c869b8",
        "Count": 2
      }
    ]
  },
  "TotalCount": 2
}
}

```

```

},
  "Type": "AwsEc2Instance",
  "Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
  "Partition": "aws",
  "Region": "us-west-2",
  "ResourceRole": "Target",
  "Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": true
  },
  "Details": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IPv4Addresses": ["1.1.1.1"],
    "IPv6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    }
  },
  "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
  ],
  "SubnetId": "PublicSubnet",
  "Type": "i3.xlarge",
  "VirtualizationType": "hvm",
  "VpcId": "TestVPCIPv6"
}
]

```

SchemaVersion

La versión del esquema para el que se está formateado un hallazgo. El valor de este campo debe ser una de las versiones publicadas oficialmente identificadas por AWS. En la versión actual, la versión del esquema AWS Security Finding Format es 2018-10-08.

Ejemplo

```
"SchemaVersion": "2018-10-08"
```

Gravedad

Define la importancia de un resultado. Para obtener más información sobre este objeto, consulte la referencia [Severity](#) de la API AWS de administración de posturas de seguridad (CSPM) de Security Hub Cloud.

Severity es a la vez un objeto de nivel superior en un resultado y está anidado debajo del objeto FindingProviderFields.

El valor del Severity objeto de nivel superior de una búsqueda solo debe actualizarse mediante la API. [BatchUpdateFindings](#)

Para proporcionar información sobre la gravedad, los proveedores de resultados deben actualizar el objeto Severity de FindingProviderFields cuando se hace una solicitud a la API [BatchImportFindings](#).

Si una BatchImportFindings solicitud de un nuevo hallazgo solo proporciona Label o solo proporcionaNormalized, Security Hub CSPM rellena automáticamente el valor del otro campo. Los Original campos Product y también pueden rellenarse.

Si el Finding.Severity objeto de nivel superior está presente pero no Finding.FindingProviderFields lo está, Security Hub CSPM crea el FindingProviderFields.Severity objeto y lo copia todo Finding.Severity object en él. Esto garantiza que los detalles originales proporcionados por el proveedor se van a retener en la estructura FindingProviderFields.Severity, incluso si se sobrescribe el objeto de nivel superior Severity.

La gravedad del hallazgo no tiene en cuenta la importancia crítica de los activos involucrados o del recurso subyacente. El nivel de importancia crítica se define como el nivel de importancia de los recursos que están asociados con el hallazgo. Por ejemplo, un recurso que está asociado a una aplicación de misión crítica tiene mayor importancia crítica frente a uno asociado a pruebas que no son de producción. Para capturar información sobre la importancia crítica de los recursos, utilice el campo Criticality.

Recomendamos utilizar la siguiente guía al traducir las puntuaciones de gravedad nativas de los resultados al valor Severity.Label en ASFF.

- **INFORMATIONAL**: Esta categoría puede incluir el resultado de PASSED, WARNING, NOT AVAILABLE o una identificación de datos confidenciales.
- **LOW**: Resultados que podrían resultar en futuros compromisos. Por ejemplo, esta categoría puede incluir vulnerabilidades, puntos débiles de configuración y contraseñas expuestas.
- **MEDIUM** – Resultados que están asociados con problemas que indican una situación de peligro activa, pero ninguna indicación de que un adversario haya completado sus objetivos. Por ejemplo, esta categoría puede incluir actividad de malware, actividad de piratería y detección de comportamientos inusual.
- **HIGH o CRITICAL** – Resultados que indican que un adversario ha completado sus objetivos, como, por ejemplo, pérdida de datos activa, situación en peligro o denegación de servicios.

Ejemplo

```
"Severity": {  
  "Label": "CRITICAL",  
  "Normalized": 90,  
  "Original": "CRITICAL"  
}
```

Título

El título de un hallazgo. Este campo puede contener texto reutilizable no específico o información específica de esta instancia del hallazgo.

En el caso de los resultados de control, este campo proporciona el título del control. Este campo no hace referencia a un estándar si activa los [resultados de control consolidados](#).

Ejemplo

```
"Title": "AWS Config should be enabled"
```

Tipos

Uno o varios tipos de hallazgos en el formato de *namespace/category/classifier* que clasifica un hallazgo. Este campo no hace referencia a un estándar si activa los [resultados de control consolidados](#).

Types debe actualizarse únicamente mediante la API. [BatchUpdateFindings](#)

Los proveedores de resultados que deseen proporcionar un valor para Types deben utilizar el atributo Types en [FindingProviderFields](#).

En la siguiente lista, las viñetas de nivel superior son espacios de nombres, las viñetas de segundo nivel son categorías y las viñetas de tercer nivel son clasificadores. Recomendamos que los proveedores de resultado utilicen espacios de nombres definidos para ayudar a ordenar y agrupar los resultados. Se recomienda el uso de las categorías y clasificadores definidos, pero no son obligatorios. Sólo el espacio de nombres Comprobaciones de software y configuración tiene clasificadores definidos.

Puede definir una ruta parcial para namespace/category/classifier. Por ejemplo, los siguientes tipos de hallazgo son válidos:

- TTPs
- TTPs/Defensa: Evasión
- TTPs/Defense Evasion/CloudTrailStopped

Las categorías de tácticas, técnicas y procedimientos (TTPs) de la siguiente lista se alinean con la MatrixTM [MITRE ATT&CK](#). Los comportamientos inusuales reflejan un comportamiento general inusual, como anomalías estadísticas generales y no están alineados con un TTP específico. Sin embargo, puede clasificar un hallazgo tanto por comportamientos inusuales como por tipos de hallazgos. TTPs

Lista de espacios de nombres, categorías y clasificadores:

- Comprobaciones de configuración y software
 - Vulnerabilidades
 - CVE
 - AWS Prácticas recomendadas de seguridad
 - Accesibilidad de red
 - Análisis del comportamiento del tiempo de ejecución
 - Estándares del sector y normativos
 - AWS Mejores prácticas de seguridad fundamentales
 - Indicadores de referencia de fortalecimiento de host de CIS
 - Punto de referencia de la AWS Fundación CIS
 - PCI-DSS

- Controles Cloud Security Alliance
- Controles ISO 90001
- Controles ISO 27001
- Controles ISO 27017
- Controles ISO 27018
- SOC 1
- SOC 2
- Controles HIPAA (EE. UU.)
- Controles 800-53 de NIST (EE. UU.)
- Controles de CSF del NIST (EE. UU.)
- Controles IRAP (Australia)
- Controles K-ISMS (Corea)
- Controles MTCS (Singapur)
- Controles FISC (Japón)
- Controles My Number Act (Japón)
- Controles ENS (España)
- Controles Cyber Essentials Plus (Reino Unido)
- Controles G-Cloud (Reino Unido)
- Controles C5 (Alemania)
- Controles IT-Grundschutz (Alemania)
- Controles del RGPD (Europa)
- Controles TISAX (Europa)
- Administración de parches
- TTPs
 - Acceso inicial
 - Ejecución
 - Persistencia
 - Escalado de privilegios
 - Evasión de defensa
- Atributos de nivel superior necesarios del ASFF
 - Acceso a credenciales

- Discovery
- Movimiento lateral
- Recopilación
- Comando y control
- Efectos
 - Exposición de datos
 - Filtración de datos
 - Destrucción de datos
 - Ataques de denegación de servicio
 - Consumo de recursos
- Comportamientos inusuales
 - Aplicación
 - Flujo de red
 - Dirección IP
 - Usuario
 - VM
 - Contenedor
 - Sin servidor
 - Proceso
 - Base de datos
 - Datos
- Identificaciones de información confidencial
 - PII
 - Contraseñas
 - Cuestiones legales
 - Datos financieros
 - Seguridad
 - Usuarios

```
"Types": [  
  "Software and Configuration Checks/Vulnerabilities/CVE"  
]
```

UpdatedAt

Indica cuándo fue la última vez que el proveedor de resultados actualizó el registro de resultado.

Esta marca de tiempo refleja la hora en que el registro de resultado se actualizó por última vez o por última vez. En consecuencia, puede diferir de la marca de tiempo `LastObservedAt`, que refleja cuándo se observó por última vez o más recientemente el evento o la vulnerabilidad.

Al actualizar el registro del hallazgo, debe actualizar esta marca temporal con la marca temporal actual. Tras la creación de un registro del resultado, las marcas temporales `CreatedAt` y `UpdatedAt` deben actualizarse a la misma marca temporal. Después de una actualización del registro del resultado, el valor de este campo debe ser el más reciente frente a todos los valores anteriores que contenía.

Tenga en cuenta que `UpdatedAt` no se puede actualizar mediante la [BatchUpdateFindings](#) operación. Solo puede actualizarlo mediante la [BatchImportFindings](#) operación.

Ejemplo

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

Atributos de nivel superior opcionales del ASFF

Los siguientes atributos de nivel superior del formato de búsqueda AWS de seguridad (ASFF) son opcionales para las búsquedas en Security Hub CSPM. Para obtener más información sobre estos atributos, consulte [AwsSecurityFinding](#) la Referencia de la API de AWS Security Hub.

Acción

El [Action](#) objeto proporciona detalles sobre una acción que afecta a un recurso o que se ha realizado en él.

Ejemplo

```
"Action": {
```

```

    "ActionType": "PORT_PROBE",
    "PortProbeAction": {
      "PortProbeDetails": [
        {
          "LocalPortDetails": {
            "Port": 80,
            "PortName": "HTTP"
          },
          "LocalIpDetails": {
            "IpAddressV4": "192.0.2.0"
          },
          "RemoteIpDetails": {
            "Country": {
              "CountryName": "Example Country"
            },
            "City": {
              "CityName": "Example City"
            },
            "GeoLocation": {
              "Lon": 0,
              "Lat": 0
            },
            "Organization": {
              "AsnOrg": "ExampleASO",
              "Org": "ExampleOrg",
              "Isp": "ExampleISP",
              "Asn": 64496
            }
          }
        }
      ],
      "Blocked": false
    }
  }
}

```

AwsAccountName

Cuenta de AWS Nombre al que se aplica el hallazgo.

Ejemplo

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

El nombre de la empresa del producto que generó el resultado. Para los hallazgos basados en el control, la empresa es AWS.

Security Hub CSPM rellena este atributo automáticamente para cada hallazgo. No puede actualizarlo mediante [BatchImportFindings](#) o [BatchUpdateFindings](#). La excepción a esto es cuando se utiliza una integración personalizada. Consulte [the section called “Integraciones de productos personalizados”](#).

Cuando se utiliza la consola CSPM de Security Hub para filtrar los resultados por nombre de empresa, se utiliza este atributo. Cuando utilizas la API CSPM de Security Hub para filtrar las conclusiones por nombre de empresa, utilizas el `aws/securityhub/CompanyName` atributo under. `ProductFields` Security Hub CSPM no sincroniza esos dos atributos.

Ejemplo

```
"CompanyName": "AWS"
```

Conformidad

El objeto [Compliance](#) normalmente proporciona detalles sobre un resultado de control, como los estándares aplicables y el estado de la comprobación de control.

Ejemplo

```
"Compliance": {
  "AssociatedStandards": [
    {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
    {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
    {"StandardsId": "standards/nist-800-53/v/5.0.0"}
  ],
  "RelatedRequirements": [
    "NIST.800-53.r5 AC-4",
    "NIST.800-53.r5 AC-4(21)",
    "NIST.800-53.r5 SC-7",
    "NIST.800-53.r5 SC-7(11)",
    "NIST.800-53.r5 SC-7(16)",
    "NIST.800-53.r5 SC-7(21)",
    "NIST.800-53.r5 SC-7(4)",
    "NIST.800-53.r5 SC-7(5)"
  ]
}
```

```

],
"SecurityControlId": "EC2.18",
"SecurityControlParameters": [
  {
    "Name": "authorizedTcpPorts",
    "Value": ["80", "443"]
  },
  {
    "Name": "authorizedUdpPorts",
    "Value": ["427"]
  }
],
"Status": "NOT_AVAILABLE",
"StatusReasons": [
  {
    "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
    "Description": "This finding has a compliance status of NOT AVAILABLE because AWS Config sent Security Hub CSPM a finding with a compliance state of Not Applicable. The potential reasons for a Not Applicable finding from Config are that (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule itself includes scenarios where Not Applicable is returned. The specific reason why Not Applicable is returned is not available in the Config rule evaluation."
  }
]
}

```

Confianza

La probabilidad de que un resultado identifique de forma precisa el comportamiento o problema que se pretendía identificar.

Confidence solo debe actualizarse mediante [BatchUpdateFindings](#).

Los proveedores de resultados que deseen proporcionar un valor para Confidence deben utilizar el atributo Confidence en FindingProviderFields. Consulte [the section called “Actualizar los resultados mediante FindingProviderFields”](#).

Confidence recibe una puntuación de 0-100 en base a una escala de proporción, donde 0 significa 0 por cien de confianza y 100 significa 100 por cien de confianza. Por ejemplo, una detección de filtración de datos en base a una desviación estadística del tráfico de red tiene una confianza mucho más baja porque no se ha verificado una filtración real.

Ejemplo

```
"Confidence": 42
```

Criticidad

El nivel de importancia que se asigna a los recursos asociados con el resultado.

Criticality solo debe actualizarse llamando a la operación de la API [BatchUpdateFindings](#). No actualice este objeto con [BatchImportFindings](#).

Los proveedores de resultados que deseen proporcionar un valor para **Criticality** deben utilizar el atributo **Criticality** en **FindingProviderFields**. Consulte [the section called “Actualizar los resultados mediante FindingProviderFields”](#).

Criticality se puntúa de 0-100, mediante una escala de proporción que solo admite números enteros. Una puntuación de 0 significa que los recursos subyacentes no tienen mucha importancia y una puntuación de 100 está reservada para los recursos de importancia vital.

Para cada recurso, tenga en cuenta lo siguiente al asignar **Criticality**:

- ¿Contiene el recurso afectado información confidencial (por ejemplo, un bucket de S3 con PII)?
- ¿Permite el recurso afectado que un adversario profundice su acceso o amplíe sus capacidades de llevar a cabo actividades malintencionadas adicionales (por ejemplo, cuenta sysadmin en peligro)?
- ¿Es el recurso un activo vital de la empresa (por ejemplo, un sistema empresarial clave que si estuviera en peligro podría afectar a los ingresos significativamente)?

Puede utilizar las siguientes directrices:

- Un recurso que habilita sistemas esenciales o que contiene un alto nivel de información confidencial puede puntuar en el intervalo de 75-100.
- Un recurso que habilita sistemas importantes (pero no esenciales) o que contiene datos moderadamente importantes puede puntuar en el intervalo de 25-75.
- Un recurso que habilita sistemas no importantes o que no contienen información confidencial debe puntuar en el intervalo de 0-24.

Ejemplo

```
"Criticality": 99
```

Detección

El `Detection` objeto proporciona detalles sobre una secuencia de ataque detectada por Amazon GuardDuty Extended Threat Detection. GuardDuty genera una secuencia de ataque que detecta cuando varios eventos se alinean con una actividad potencialmente sospechosa. Para recibir los resultados de la secuencia de GuardDuty ataques en AWS Security Hub Cloud Security Posture Management (CSPM), debe tener la GuardDuty opción habilitada en su cuenta. Para obtener más información, consulte [Amazon GuardDuty Extended Threat Detection](#) en la Guía del GuardDuty usuario de Amazon.

Ejemplo

```
"Detection": {
  "Sequence": {
    "Uid": "111111111111-184ec3b9-cf8d-452d-9aad-f5bdb7afb010",
    "Actors": [{
      "Id": "USER:AROA987654321EXAMPLE:i-b188560f:1234567891",
      "Session": {
        "Uid": "1234567891",
        "MfAStatus": "DISABLED",
        "CreatedTime": "1716916944000",
        "Issuer": "arn:aws:s3::amzn-s3-demo-destination-bucket"
      },
      "User": {
        "CredentialUid": "ASIAIOSFODNN7EXAMPLE",
        "Name": "ec2_instance_role_production",
        "Type": "AssumedRole",
        "Uid": "AROA987654321EXAMPLE:i-b188560f",
        "Account": {
          "Uid": "AccountId",
          "Name": "AccountName"
        }
      }
    }
  ],
  "Endpoints": [{
    "Id": "EndpointId",
    "Ip": "203.0.113.1",
    "Domain": "example.com",
    "Port": 4040,
    "Location": {
```

```
    "City": "New York",
    "Country": "US",
    "Lat": 40.7123,
    "Lon": -74.0068
  },
  "AutonomousSystem": {
    "Name": "AnyCompany",
    "Number": 64496
  },
  "Connection": {
    "Direction": "INBOUND"
  }
}],
"Signals": [{
  "Id": "arn:aws:guardduty:us-east-1:123456789012:detector/
d0bfe135ab8b4dd8c3eaae7df9900073/finding/535a382b1bcc44d6b219517a29058fb7",
  "Title": "Someone ran a penetration test tool on your account.",
  "ActorIds": ["USER:AR0A987654321EXAMPLE:i-b188560f:1234567891"],
  "Count": 19,
  "FirstSeenAt": 1716916943000,
  "SignalIndicators": [
    {
      "Key": "ATTACK_TACTIC",
      "Title": "Attack Tactic",
      "Values": [
        "Impact"
      ]
    },
    {
      "Key": "HIGH_RISK_API",
      "Title": "High Risk Api",
      "Values": [
        "s3:DeleteObject"
      ]
    },
    {
      "Key": "ATTACK_TECHNIQUE",
      "Title": "Attack Technique",
      "Values": [
        "Data Destruction"
      ]
    }
  ],
  "LastSeenAt": 1716916944000,
```

```

    "Name": "Test:IAMUser/KaliLinux",
    "ResourceIds": [
      "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    ],
    "Type": "FINDING"
  }],
  "SequenceIndicators": [
    {
      "Key": "ATTACK_TACTIC",
      "Title": "Attack Tactic",
      "Values": [
        "Discovery",
        "Exfiltration",
        "Impact"
      ]
    },
    {
      "Key": "HIGH_RISK_API",
      "Title": "High Risk Api",
      "Values": [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBuckets",
        "s3:ListObjects"
      ]
    },
    {
      "Key": "ATTACK_TECHNIQUE",
      "Title": "Attack Technique",
      "Values": [
        "Cloud Service Discovery",
        "Data Destruction"
      ]
    }
  ]
}

```

FindingProviderFields

FindingProviderFields incluye los siguientes atributos:

- Confidence

- Criticality
- RelatedFindings
- Severity
- Types

Los campos anteriores están anidados debajo del objeto `FindingProviderFields`, pero tienen análogos del mismo nombre que los campos del ASFF de nivel superior. Cuando un proveedor de búsquedas envía un nuevo hallazgo al Security Hub CSPM, Security Hub CSPM rellena el `FindingProviderFields` objeto automáticamente si está vacío en función de los campos de nivel superior correspondientes.

La búsqueda de proveedores se puede actualizar `FindingProviderFields` mediante el [BatchImportFindings](#) funcionamiento de la API CSPM de Security Hub. Los proveedores de resultados no pueden actualizar este objeto mediante [BatchUpdateFindings](#).

Para obtener más información sobre cómo el CSPM de Security Hub gestiona las actualizaciones desde `FindingProviderFields` y `BatchImportFindings` hacia los atributos de nivel superior correspondientes, consulte. [the section called "Actualizar los resultados mediante FindingProviderFields"](#)

Los clientes pueden actualizar los campos de nivel superior mediante la operación `BatchUpdateFindings`. Los clientes no pueden actualizar `FindingProviderFields`.

Ejemplo

```
"FindingProviderFields": {
  "Confidence": 42,
  "Criticality": 99,
  "RelatedFindings": [
    {
      "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000"
    }
  ],
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

```
}
```

FirstObservedAt

Indica cuándo se observó por primera vez el posible problema o evento de seguridad detectado por un hallazgo.

Esta marca de tiempo especifica cuándo se observó por primera vez el evento o la vulnerabilidad. Por lo tanto, puede diferir de la `CreatedAt` marca de tiempo, que refleja cuándo se creó este registro de hallazgos.

La marca temporal debe permanecer inmutable entre actualizaciones del registro del resultado, pero se puede actualizar si se ha determinado una marca temporal más precisa.

Ejemplo

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

Indica cuándo el producto de hallazgos de seguridad detectó por última vez el posible problema o evento de seguridad detectado por un hallazgo.

Esta marca de tiempo especifica cuándo se observó por última vez o más recientemente el evento o la vulnerabilidad. Por lo tanto, puede diferir de la marca de tiempo `UpdatedAt`, que refleja cuándo se actualizó este registro de resultados por última vez.

Puede proporcionar esta marca temporal, pero no es necesaria tras la primera observación. Si rellena este campo en la primera observación, la marca de tiempo debe ser la misma que la marca de tiempo. `FirstObservedAt` Debe actualizar este campo para reflejar la marca temporal observada más recientemente o por última vez cada vez se observa un resultado.

Ejemplo

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

Malware

El objeto [Malware](#) proporciona una lista de malware relacionado con un hallazgo.

Ejemplo

```
"Malware": [  
  {  
    "Name": "Stringler",  
    "Type": "COIN_MINER",  
    "Path": "/usr/sbin/stringler",  
    "State": "OBSERVED"  
  }  
]
```

Network (Retired)

El objeto [Network](#) brinda información relacionada con la red de un resultado.

Este objeto se ha retirado. Para proporcionar estos datos, puede asignar los datos a un recurso en [Resources](#) o utilizar el objeto [Action](#).

Ejemplo

```
"Network": {  
  "Direction": "IN",  
  "OpenPortRange": {  
    "Begin": 443,  
    "End": 443  
  },  
  "Protocol": "TCP",  
  "SourceIPv4": "1.2.3.4",  
  "SourceIPv6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",  
  "SourcePort": "42",  
  "SourceDomain": "example1.com",  
  "SourceMac": "00:0d:83:b1:c0:8e",  
  "DestinationIPv4": "2.3.4.5",  
  "DestinationIPv6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",  
  "DestinationPort": "80",  
  "DestinationDomain": "example2.com"  
}
```

NetworkPath

El objeto [NetworkPath](#) proporciona información sobre una ruta de red relacionada con un resultado. Cada entrada en [NetworkPath](#) representa un componente de la ruta.

Ejemplo

```

"NetworkPath" : [
  {
    "ComponentId": "abc-01a234bc56d8901ee",
    "ComponentType": "AWS::EC2::InternetGateway",
    "Egress": {
      "Destination": {
        "Address": [ "192.0.2.0/24" ],
        "PortRanges": [
          {
            "Begin": 443,
            "End": 443
          }
        ]
      },
      "Protocol": "TCP",
      "Source": {
        "Address": ["203.0.113.0/24"]
      }
    },
    "Ingress": {
      "Destination": {
        "Address": [ "198.51.100.0/24" ],
        "PortRanges": [
          {
            "Begin": 443,
            "End": 443
          }
        ]
      },
      "Protocol": "TCP",
      "Source": {
        "Address": [ "203.0.113.0/24" ]
      }
    }
  }
]

```

Nota

El objeto [Note](#) especifica una nota definida por el usuario que se puede añadir a un resultado.

Un proveedor de hallazgos puede proporcionar una nota inicial para un hallazgo, pero después no puede agregar más notas. Solo puede actualizar una nota con [BatchUpdateFindings](#).

Ejemplo

```
"Note": {
  "Text": "Don't forget to check under the mat.",
  "UpdatedBy": "jsmith",
  "UpdatedAt": "2018-08-31T00:15:09Z"
}
```

PatchSummary

El objeto [PatchSummary](#) proporciona un resumen del estado de conformidad del parche de una instancia con respecto a un estándar de cumplimiento seleccionado.

Ejemplo

```
"PatchSummary" : {
  "FailedCount" : 0,
  "Id" : "pb-123456789098",
  "InstalledCount" : 100,
  "InstalledOtherCount" : 1023,
  "InstalledPendingReboot" : 0,
  "InstalledRejectedCount" : 0,
  "MissingCount" : 100,
  "Operation" : "Install",
  "OperationEndTime" : "2018-09-27T23:39:31Z",
  "OperationStartTime" : "2018-09-27T23:37:31Z",
  "RebootOption" : "RebootIfNeeded"
}
```

Proceso

El objeto [Process](#) proporciona detalles relacionados con el proceso acerca del resultado.

Ejemplo:

```
"Process": {
  "LaunchedAt": "2018-09-27T22:37:31Z",
  "Name": "syslogd",
  "ParentPid": 56789,
  "Path": "/usr/sbin/syslogd",
  "Pid": 12345,
  "TerminatedAt": "2018-09-27T23:37:31Z"
```

```
}
```

ProcessedAt

Indica cuándo Security Hub CSPM recibió un hallazgo y comenzó a procesarlo.

Esto difiere de `CreatedAt` y `UpdatedAt`, que son marcas temporales obligatorias relacionadas con la interacción del proveedor del hallazgo con el problema de seguridad y el hallazgo. La `ProcessedAt` marca de tiempo indica cuándo Security Hub CSPM comienza a procesar un hallazgo. Una vez finalizado el procesamiento, aparece un hallazgo en la cuenta de un usuario.

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

Un tipo de datos en el que los productos de análisis de seguridad pueden incluir detalles adicionales específicos de la solución que no forman parte del formato de análisis de AWS seguridad definido.

Para los hallazgos generados por los controles CSPM de Security Hub, `ProductFields` incluye información sobre el control. Consulte [the section called “Generación y actualización de los resultados de control”](#).

Este campo no debe contener datos redundantes ni debe contener datos que entren en conflicto con los campos del formato de búsqueda AWS de seguridad.

El prefijo `aws/` representa un espacio de nombres reservado únicamente para AWS productos y servicios y no debe enviarse junto con los resultados de integraciones de terceros.

Aunque no es necesario, los productos deben formatear los nombres de los campos como `company-id/product-id/field-name`, donde el `company-id` y el `product-id` coinciden con los suministrados en el `ProductArn` del hallazgo.

Los campos que hacen referencia `Archival` se utilizan cuando Security Hub CSPM archiva un hallazgo existente. Por ejemplo, Security Hub CSPM archiva las conclusiones existentes al deshabilitar un control o estándar y al activar o desactivar las [conclusiones de los controles consolidados](#).

Este campo también puede incluir información sobre el estándar que incluye el control que produjo el resultado.

Ejemplo

```
"ProductFields": {
  "API", "DeleteTrail",
  "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because consolidated control findings has been turned on or off. This causes findings in the previous state to be archived when new findings are being generated.",
  "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
  "aws/inspector/AssessmentTargetName": "My prod env",
  "aws/inspector/AssessmentTemplateName": "My daily CVE assessment",
  "aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",
  "generico/secure-pro/Action.Type", "AWS_API_CALL",
  "generico/secure-pro/Count": "6",
  "Service_Name": "cloudtrail.amazonaws.com"
}
```

ProductName

Proporciona el nombre del producto que generó el resultado. Para los hallazgos basados en el control, el nombre del producto es Security Hub CSPM.

Security Hub CSPM rellena este atributo automáticamente para cada hallazgo. No puede actualizarlo mediante [BatchImportFindings](#) o [BatchUpdateFindings](#). La excepción a esto es cuando se utiliza una integración personalizada. Consulte [the section called “Integraciones de productos personalizados”](#).

Cuando se utiliza la consola CSPM de Security Hub para filtrar los resultados por nombre de producto, se utiliza este atributo.

Cuando utilizas la API CSPM de Security Hub para filtrar los resultados por nombre de producto, utilizas el `aws/securityhub/ProductName` atributo under. `ProductFields`

Security Hub CSPM no sincroniza esos dos atributos.

RecordState

El estado de registro de un a resultado.

De forma predeterminada, los hallazgos generados inicialmente por un servicio se consideran ACTIVE.

El estado ARCHIVED indica que un hallazgo estará oculto a la vista. Los hallazgos archivados no se eliminan inmediatamente. Puede buscar, examinar e informar sobre ellos. Security Hub CSPM archiva automáticamente las conclusiones basadas en el control si se elimina el recurso asociado, el recurso no existe o el control está deshabilitado.

RecordState está diseñado para buscar proveedores y solo se puede actualizar mediante la operación. [BatchImportFindings](#). No se puede actualizar mediante la [BatchUpdateFindings](#) operación.

Para hacer un seguimiento del estado de la investigación sobre un resultado, utilice [Workflow](#) en lugar de RecordState.

Si el estado del registro cambia de ARCHIVED a ACTIVE y el estado del flujo de trabajo de la búsqueda es NOTIFIED o RESOLVED, Security Hub CSPM cambia automáticamente el estado del flujo de trabajo a. NEW

Ejemplo

```
"RecordState": "ACTIVE"
```

Región

Especifica Región de AWS desde dónde se generó la búsqueda.

Security Hub CSPM rellena este atributo automáticamente para cada hallazgo. No puede actualizarlo mediante [BatchImportFindings](#) o [BatchUpdateFindings](#).

Ejemplo

```
"Region": "us-west-2"
```

RelatedFindings

Proporciona una lista de resultados relacionados con el resultado actual.

RelatedFindings solo debe actualizarse con la operación de la API [BatchUpdateFindings](#). No debe actualizar este objeto con [BatchImportFindings](#).

Para las solicitudes [BatchImportFindings](#), los proveedores de resultados deben utilizar el objeto RelatedFindings en [FindingProviderFields](#).

Para ver las descripciones de RelatedFindings los atributos, consulte la referencia [RelatedFinding](#) de la API AWS de administración de posturas de seguridad (CSPM) de Security Hub Cloud.

Ejemplo

```
"RelatedFindings": [
  { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
    "Id": "123e4567-e89b-12d3-a456-426655440000" },
  { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
    "Id": "AcmeNerfHerder-111111111111-x189dx7824" }
]
```

RiskAssessment

Ejemplo

```
"RiskAssessment": {
  "Posture": {
    "FindingTotal": 4,
    "Indicators": [
      {
        "Type": "Reachability",
        "Findings": [
          {
            "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/1234567890abcdef0",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
            "Title": "Finding title"
          },
          {
            "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/abcdef01234567890",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
            "Title": "Finding title"
          }
        ]
      },
      {
        "Type": "Vulnerability",
```

```

      "Findings": [
        {
          "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/021345abcdef6789",
          "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
          "Title": "Finding title"
        },
        {
          "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/021345ghijkl6789",
          "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
          "Title": "Finding title"
        }
      ]
    }
  ]
}

```

Corrección

El objeto [Remediation](#) proporciona información sobre los pasos de corrección recomendados para solucionar el hallazgo.

Ejemplo

```

"Remediation": {
  "Recommendation": {
    "Text": "For instructions on how to fix this issue, see the AWS Security Hub Cloud Security Posture Management (CSPM) documentation for EC2.2.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"
  }
}

```

Muestra

Especifica si el resultado es un resultado de muestra.

```
"Sample": true
```

SourceUrl

El objeto `SourceUrl` brinda una URL que enlaza a una página sobre el resultado actual en el producto de resultados.

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

El objeto [ThreatIntelIndicator](#) brinda detalles de información de amenazas que están relacionados con un resultado.

Ejemplo

```
"ThreatIntelIndicators": [  
  {  
    "Category": "BACKDOOR",  
    "LastObservedAt": "2018-09-27T23:37:31Z",  
    "Source": "Threat Intel Weekly",  
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",  
    "Type": "IPV4_ADDRESS",  
    "Value": "8.8.8.8",  
  }  
]
```

Amenazas

El objeto [Threats](#) proporciona detalles sobre la amenaza detectada por un resultado.

Ejemplo

```
"Threats": [{  
  "FilePaths": [{  
    "FileName": "b.txt",  
    "FilePath": "/tmp/b.txt",  
    "Hash": "sha256",  
    "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"  
  }],  
  "ItemCount": 3,  
  "Name": "Iot.linux.mirai.vwisi",  
}
```

```
"Severity": "HIGH"
}]
```

UserDefinedFields

Una lista de pares de cadenas de nombre/valor que están asociados con el resultado. Son campos definidos por el usuario y personalizados que se añaden a un hallazgo. Estos campos se pueden generar de forma automática a través de su configuración específica.

Los proveedores de resultados no deben utilizar este campo para los datos que genera el producto. En su lugar, los proveedores de búsqueda pueden utilizar el `ProductFields` campo para los datos que no se asignen a ningún campo estándar del formato AWS de búsqueda de seguridad.

Estos campos solo se pueden actualizar con [BatchUpdateFindings](#).

Ejemplo

```
"UserDefinedFields": {
  "reviewedByCio": "true",
  "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

Brinda la veracidad de un resultado. Los productos de resultados pueden proporcionar el valor UNKNOWN para este campo. Un producto de resultados puede proporcionar este valor para este campo si hay un valor analógico significativo en el sistema del producto de resultados. Este campo suele ser rellenado por una determinación o acción del usuario después de que haya investigado un resultado.

Un proveedor de hallazgos puede proporcionar un valor inicial para este atributo, pero después no puede actualizarlo. Solo puede actualizar este atributo mediante [BatchUpdateFindings](#).

```
"VerificationState": "Confirmed"
```

Vulnerabilidades

El objeto [Vulnerabilities](#) proporciona una lista de vulnerabilidades asociadas a un resultado.

Ejemplo

```

"Vulnerabilities" : [
  {
    "CodeVulnerabilities": [{
      "Cwes": [
        "CWE-798",
        "CWE-799"
      ],
      "FilePath": {
        "EndLine": 421,
        "FileName": "package-lock.json",
        "FilePath": "package-lock.json",
        "StartLine": 420
      },
      "SourceArn": "arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-Extension:114"
    }],
    "Cvss": [
      {
        "BaseScore": 4.7,
        "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
        "Version": "V3"
      },
      {
        "BaseScore": 4.7,
        "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
        "Version": "V2"
      }
    ],
    "EpssScore": 0.015,
    "ExploitAvailable": "YES",
    "FixAvailable": "YES",
    "Id": "CVE-2020-12345",
    "LastKnownExploitAt": "2020-01-16T00:01:35Z",
    "ReferenceUrls": [
      "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",
      "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
    ],
    "RelatedVulnerabilities": ["CVE-2020-12345"],
    "Vendor": {
      "Name": "Alas",
      "Url": "https://alas.aws.amazon.com/ALAS-2020-1337.html",
      "VendorCreatedAt": "2020-01-16T00:01:43Z",

```

```

        "VendorSeverity": "Medium",
        "VendorUpdatedAt": "2020-01-16T00:01:43Z"
    },
    "VulnerablePackages": [
        {
            "Architecture": "x86_64",
            "Epoch": "1",
            "FilePath": "/tmp",
            "FixedInVersion": "0.14.0",
            "Name": "openssl",
            "PackageManager": "OS",
            "Release": "16.amzn2.0.3",
            "Remediation": "Update aws-crt to 0.14.0",
            "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
            "SourceLayerHash":
"sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
            "Version": "1.0.2k"
        }
    ]
}
]

```

Flujo de trabajo

El objeto [Workflow](#) proporciona información sobre el estado de la investigación de un hallazgo.

Este campo está pensado para que los clientes lo utilicen con herramientas de corrección, orquestación y emisión de tickets. No está destinado a proveedores de hallazgos.

Solo puede actualizar el campo Workflow con [BatchUpdateFindings](#). Los clientes también pueden actualizarlo desde la consola. Consulte [the section called “Configuración del estado de flujo de trabajo de los resultados”](#).

Ejemplo

```

"Workflow": {
    "Status": "NEW"
}

```

WorkflowState (Retirado)

Este objeto está retirado y se ha sustituido por el campo Status del objeto Workflow.

Este campo proporciona el estado del flujo de trabajo de un resultado. Los productos de hallazgos puede proporcionar el valor NEW para este campo. Un producto de hallazgos puede proporcionar este valor si hay un valor analógico significativo en el sistema del producto de hallazgos.

Ejemplo

```
"WorkflowState": "NEW"
```

Objeto Resources del ASFF

En el formato AWS de búsqueda de seguridad (ASFF), el Resources objeto proporciona información sobre los recursos involucrados en una búsqueda. Contiene una matriz de hasta 32 objetos de recursos. Para determinar el formato de los nombres de los recursos, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#). Para ver ejemplos de cada objeto de recurso, seleccione un recurso en la siguiente lista.

Temas

- [Atributos de recursos en el ASFF](#)
- [Recursos de AwsAmazonMQ en el ASFF](#)
- [Recursos de AwsApiGateway en el ASFF](#)
- [Recursos de AwsAppSync en el ASFF](#)
- [Recursos de AwsAthena en el ASFF](#)
- [Recursos de AwsAutoScaling en el ASFF](#)
- [Recursos de AwsBackup en el ASFF](#)
- [Recursos de AwsCertificateManager en el ASFF](#)
- [Recursos de AwsCloudFormation en el ASFF](#)
- [Recursos de AwsCloudFront en el ASFF](#)
- [Recursos de AwsCloudTrail en el ASFF](#)
- [Recursos de AwsCloudWatch en el ASFF](#)
- [Recursos de AwsCodeBuild en el ASFF](#)
- [Recursos de AwsDms en el ASFF](#)
- [Recursos de AwsDynamoDB en el ASFF](#)
- [Recursos de AwsEc2 en el ASFF](#)

- [Recursos de AwsEcr en el ASFF](#)
- [Recursos de AwsEcs en el ASFF](#)
- [Recursos de AwsEfs en el ASFF](#)
- [Recursos de AwsEks en el ASFF](#)
- [Recursos de AwsElasticBeanstalk en el ASFF](#)
- [Recursos de AwsElasticSearch en el ASFF](#)
- [Recursos de AwsElb en el ASFF](#)
- [Recursos de AwsEventBridge en el ASFF](#)
- [Recursos de AwsGuardDuty en el ASFF](#)
- [Recursos de AwsIam en el ASFF](#)
- [Recursos de AwsKinesis en el ASFF](#)
- [Recursos de AwsKms en el ASFF](#)
- [AwsLambda](#)
- [Recursos de AwsMsk en el ASFF](#)
- [Recursos de AwsNetworkFirewall en el ASFF](#)
- [Recursos de AwsOpenSearchService en el ASFF](#)
- [Recursos de AwsRds en el ASFF](#)
- [Recursos de AwsRedshift en el ASFF](#)
- [Recursos de AwsRoute53 en el ASFF](#)
- [Recursos de AwsS3 en el ASFF](#)
- [Recursos de AwsSageMaker en el ASFF](#)
- [Recursos de AwsSecretsManager en el ASFF](#)
- [Recursos de AwsSns en el ASFF](#)
- [Recursos de AwsSqs en el ASFF](#)
- [Recursos de AwsSsm en el ASFF](#)
- [Recursos de AwsStepFunctions en el ASFF](#)
- [Recursos de AwsWaf en el ASFF](#)
- [Recursos de AwsXray en el ASFF](#)
- [Objeto Container del ASFF](#)
- [Objeto Other del ASFF](#)

Atributos de recursos en el ASFF

A continuación, se muestran descripciones y ejemplos del Resources objeto en el formato AWS de búsqueda de seguridad (ASFF). Para obtener más información acerca de estos campos, consulte [Recursos](#).

ApplicationArn

Identifica el nombre de recurso de Amazon (ARN) de la aplicación implicada en el resultado.

Ejemplo

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/SampleApp/1234567890abcdef0"
```

ApplicationName

Identifica el nombre de la aplicación implicada en el resultado.

Ejemplo

```
"ApplicationName": "SampleApp"
```

DataClassification

El campo [DataClassification](#) proporciona información sobre los datos confidenciales que se detectaron en el recurso.

Ejemplo

```
"DataClassification": {
  "DetailedResultsLocation": "Path_to_Folder_Or_File",
  "Result": {
    "MimeType": "text/plain",
    "SizeClassified": 2966026,
    "AdditionalOccurrences": false,
    "Status": {
      "Code": "COMPLETE",
      "Reason": "Unsupportedfield"
    },
  },
  "SensitiveData": [
    {
      "Category": "PERSONAL_INFORMATION",
```

```

"Detections": [
  {
    "Count": 34,
    "Type": "GE_PERSONAL_ID",
    "Occurrences": {
      "LineRanges": [
        {
          "Start": 1,
          "End": 10,
          "StartColumn": 20
        }
      ],
      "Pages": [],
      "Records": [],
      "Cells": []
    }
  },
  {
    "Count": 59,
    "Type": "EMAIL_ADDRESS",
    "Occurrences": {
      "Pages": [
        {
          "PageNumber": 1,
          "OffsetRange": {
            "Start": 1,
            "End": 100,
            "StartColumn": 10
          },
          "LineRange": {
            "Start": 1,
            "End": 100,
            "StartColumn": 10
          }
        }
      ]
    }
  },
  {
    "Count": 2229,
    "Type": "URL",
    "Occurrences": {
      "LineRanges": [
        {

```

```

        "Start": 1,
        "End": 13
      }
    ]
  },
  {
    "Count": 13826,
    "Type": "NameDetection",
    "Occurrences": {
      "Records": [
        {
          "RecordIndex": 1,
          "JsonPath": "$.ssn.value"
        }
      ]
    }
  },
  {
    "Count": 32,
    "Type": "AddressDetection"
  }
],
"TotalCount": 32
}
],
"CustomDataIdentifiers": {
  "Detections": [
    {
      "Arn": "1712be25e7c7f53c731fe464f1c869b8",
      "Name": "1712be25e7c7f53c731fe464f1c869b8",
      "Count": 2,
    }
  ],
  "TotalCount": 2
}
}

```

Detalles

El campo [Details](#) proporciona información adicional sobre un único recurso que utiliza los objetos adecuados. Cada recurso debe facilitarse en un objeto de recurso independiente en el objeto `Resources`.

Tenga en cuenta que si el tamaño del resultado supera el máximo de 240 KB, el objeto `Details` se elimina del resultado. Para ver los resultados de control que utilizan AWS Config reglas, puede ver los detalles del recurso en la AWS Config consola.

Security Hub brinda un conjunto de detalles de recursos disponibles para los tipos de recursos admitidos. Estos detalles corresponden a los valores del objeto `Type`. Siempre que sea posible, utilice los tipos proporcionados.

Por ejemplo, si el recurso es un bucket de S3, entonces establezca el recurso `Type` en `AwsS3Bucket` y proporcione los detalles del recurso en el objeto [AwsS3Bucket](#).

El objeto [Other](#) le permite proporcionar campos y valores personalizados. Utilice el objeto `Other` en los siguientes casos:

- El tipo de recurso (el valor del recurso `Type`) no tiene un objeto con detalles correspondiente. Para proporcionar detalles sobre el recurso, utilice el objeto [Other](#).
- El objeto del tipo de recurso no incluye todos los campos que desea rellenar. En este caso, utilice el objeto de detalles del tipo de recurso para rellenar los campos disponibles. Utilice el objeto `Other` para rellenar los campos que no están en el subcampo específico de ese objeto.
- El tipo de recurso no es uno de los tipos proporcionados. En este caso, establezca `Resource.Type` en `Other` y utilice el objeto `Other` para rellenar los detalles.

Ejemplo

```
"Details": {
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IPv4Addresses": ["1.1.1.1"],
    "IPv6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
```



```

    "HttpProtocolIpv6": "enabled",
    "HttpPutResponseHopLimit": 1,
    "HttpTokens": "optional",
    "InstanceMetadataTags": "disabled"
  },
  "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
  ],
  "SubnetId": "PublicSubnet",
  "Type": "i3.xlarge",
  "VirtualizationType": "hvm",
  "VpcId": "TestVPCIPv6"
},
"AwsS3Bucket": {
  "OwnerId": "da4d66eac431652a4d44d490a00500bde52c97d235b7b4752f9f688566fe6de",
  "OwnerName": "acmes3bucketowner"
},
"Other": { "LightPen": "blinky", "SerialNo": "1234abcd" }
}

```

Id

El identificador para el tipo de recurso determinado.

Para AWS los recursos que se identifican mediante Amazon Resource Names (ARNs), este es el ARN.

En el AWS caso de los recursos que faltan ARNs, este es el identificador definido por el AWS servicio que creó el recurso.

En el caso de AWS los que no son recursos, se trata de un identificador único que se asocia al recurso.

Ejemplo

```
"Id": "arn:aws:s3:::amzn-s3-demo-bucket"
```

Partición

La partición en la que se encuentra el recurso. Una partición es un grupo de Regiones de AWS. Cada una Cuenta de AWS tiene el alcance de una partición.

Se admiten las siguientes particiones:

- aws – Regiones de AWS
- aws-cn: regiones de China
- aws-us-gov – AWS GovCloud (US) Region

Ejemplo

```
"Partition": "aws"
```

Región

El código de la Región de AWS ubicación de este recurso. Para ver una lista de códigos de regiones, consulte [Puntos de conexión regionales](#).

Ejemplo

```
"Region": "us-west-2"
```

ResourceRole

Identifica la característica del recurso en el resultado. Un recurso es el objetivo de la actividad de resultado o el actor que realizó la actividad.

Ejemplo

```
"ResourceRole": "target"
```

Etiquetas

Este campo proporciona información sobre la clave y el valor de la etiqueta del recurso implicado en un resultado. Puede etiquetar [los recursos compatibles con](#) el GetResources funcionamiento de la API de AWS Resource Groups etiquetado. Security Hub llama a esta operación a través del [rol vinculado al servicio](#) y recupera las etiquetas de recursos si el Resource . Id campo AWS Security Finding Format (ASFF) se rellena con el ARN del recurso. AWS Se omiten los recursos no válidos. IDs

Puede agregar etiquetas de recursos a los resultados que ingiera Security Hub, incluidos los resultados de Servicios de AWS integrados y productos de terceros.

Cuando agrega etiquetas, se indican las etiquetas que estaban asociadas con un recurso en el momento en que se procesó el resultado. Puede incluir el atributo `Tags` solamente para los recursos que tienen una etiqueta asociada. Si un recurso no tiene etiqueta asociada, no incluya un atributo `Tags` en el hallazgo.

La inclusión de etiquetas de recursos en los resultados elimina la necesidad de crear canalizaciones de enriquecimiento de datos o enriquecer manualmente los metadatos de los resultados de seguridad. También puede usar etiquetas para buscar o filtrar los resultados e información y crear [reglas de automatización](#).

Para obtener información sobre las restricciones que se aplican a las etiquetas, consulte [Tag naming limits and requirements](#).

En este campo, solo puede proporcionar las etiquetas que existan en un AWS recurso. Para proporcionar datos que no estén definidos en el formato de comprobación AWS de seguridad, utilice el subcampo de `Other` detalles.

Ejemplo

```
"Tags": {
  "billingCode": "Lotus-1-2-3",
  "needsPatching": "true"
}
```

Tipo

Tipo de recurso del que se proporcionan detalles.

Siempre que sea posible, utilice uno de los tipos de recursos proporcionados, como `AwsEc2Instance` o `AwsS3Bucket`.

Si el tipo de recurso no coincide con ninguno de los tipos de recursos proporcionados, establezca el recurso `Type` en `Other` y utilice el subcampo de detalles `Other` para rellenar los detalles.

Los valores admitidos se muestran en [Recursos](#).

Ejemplo

```
"Type": "AwsS3Bucket"
```

Recursos de AwsAmazonMQ en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los AwsAmazonMQ recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsAmazonMQBroker

AwsAmazonMQBroker proporciona información acerca de un agente de Amazon MQ, que es un entorno de agente de mensajes que se ejecuta en Amazon MQ.

En el ejemplo siguiente se muestra el ASFF para el objeto AwsAmazonMQBroker. Para ver las descripciones de los atributos AwsAmazonMQBroker, consulte [AwsAmazonMQBroker](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsAmazonMQBroker": {
  "AutoMinorVersionUpgrade": true,
  "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "BrokerName": "TestBroker",
  "Configuration": {
    "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "Revision": 1
  },
  "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
  "EncryptionOptions": {
    "UseAwsOwnedKey": true
  },
  "EngineType": "ActiveMQ",
  "EngineVersion": "5.17.2",
  "HostInstanceType": "mq.t2.micro",
  "Logs": {
    "Audit": false,
    "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/
audit",
    "General": false,
    "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111/general"
```

```
    },
    "MaintenanceWindowStartTime": {
      "DayOfWeek": "MONDAY",
      "TimeOfDay": "22:00",
      "TimeZone": "UTC"
    },
    "PubliclyAccessible": true,
    "SecurityGroups": [
      "sg-021345abcdef6789"
    ],
    "StorageType": "efs",
    "SubnetIds": [
      "subnet-1234567890abcdef0",
      "subnet-abcdef01234567890"
    ],
    "Users": [
      {
        "Username": "admin"
      }
    ]
  }
}
```

Recursos de AwsApiGateway en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsApiGateway los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsApiGatewayRestApi

El objeto `AwsApiGatewayRestApi` contiene información sobre una API de REST de la versión 1 de Amazon API Gateway.

A continuación, se muestra un ejemplo de resultado de `AwsApiGatewayRestApi` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsApiGatewayRestApi`, consulte [AwsApiGatewayRestApiDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
AwsApiGatewayRestApi: {
```

```

    "Id": "exampleapi",
    "Name": "Security Hub",
    "Description": "AWS Security Hub",
    "CreateDate": "2018-11-18T10:20:05-08:00",
    "Version": "2018-10-26",
    "BinaryMediaTypes" : ["-*~1*"],
    "MinimumCompressionSize": 1024,
    "ApiKeySource": "AWS_ACCOUNT_ID",
    "EndpointConfiguration": {
        "Types": [
            "REGIONAL"
        ]
    }
}

```

AwsApiGatewayStage

El objeto `AwsApiGatewayStage` proporciona información sobre una etapa de Amazon API Gateway de la versión 1.

A continuación, se muestra un ejemplo de resultado de `AwsApiGatewayStage` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsApiGatewayStage`, consulte [AwsApiGatewayStageDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsApiGatewayStage": {
    "DeploymentId": "n7hlmf",
    "ClientCertificateId": "a1b2c3",
    "StageName": "Prod",
    "Description" : "Stage Description",
    "CacheClusterEnabled": false,
    "CacheClusterSize" : "1.6",
    "CacheClusterStatus": "NOT_AVAILABLE",
    "MethodSettings": [
        {
            "MetricsEnabled": true,
            "LoggingLevel": "INFO",
            "DataTraceEnabled": false,
            "ThrottlingBurstLimit": 100,
            "ThrottlingRateLimit": 5.0,
            "CachingEnabled": false,

```

```

        "CacheTtlInSeconds": 300,
        "CacheDataEncrypted": false,
        "RequireAuthorizationForCacheControl": true,
        "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
        "HttpMethod": "POST",
        "ResourcePath": "/echo"
    }
],
"Variables": {"test": "value"},
"DocumentationVersion": "2.0",
"AccessLogSettings": {
    "Format": "{\\"requestId\\": \\"$context.requestId\\", \\"extendedRequestId
\\": \\"$context.extendedRequestId\\", \\"ownerAccountId\\": \\"$context.accountId\\",
\\": \\"$context.identity.caller\\", \\"httpMethod\\": \\"$context.httpMethod\\", \\"resourcePath
\\": \\"$context.resourcePath\\", \\"status\\": \\"$context.status\\", \\"requestTime
\\": \\"$context.requestTime\\", \\"responseLatencyMs\\": \\"$context.responseLatency
\\", \\"errorMessage\\": \\"$context.error.message\\", \\"errorResponseType\\":
\\": \\"$context.error.responseType\\", \\"apiId\\": \\"$context.apiId\\", \\"awsEndpointRequestId
\\": \\"$context.awsEndpointRequestId\\", \\"domainName\\": \\"$context.domainName\\", \\"stage
\\": \\"$context.stage\\", \\"xrayTraceId\\": \\"$context.xrayTraceId\\", \\"sourceIp\\":
\\": \\"$context.identity.sourceIp\\", \\"user\\": \\"$context.identity.user\\", \\"userAgent
\\": \\"$context.identity.userAgent\\", \\"userArn\\": \\"$context.identity.userArn\\",
\\": \\"$context.integrationLatency\\", \\"integrationStatus
\\": \\"$context.integrationStatus\\", \\"authorizerIntegrationLatency\\":
\\": \\"$context.authorizer.integrationLatency\\" }",
    "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
},
"CanarySettings": {
    "PercentTraffic": 0.0,
    "DeploymentId": "ul73s8",
    "StageVariableOverrides" : [
        "String" : "String"
    ],
    "UseStageCache": false
},
"TracingEnabled": false,
"CreatedDate": "2018-07-11T10:55:18-07:00",
"LastUpdatedDate": "2020-08-26T11:51:04-07:00",
"WebAclArn" : "arn:aws:waf-regional:us-west-2:111122223333:webacl/
cb606bd8-5b0b-4f0b-830a-dd304e48a822"
}

```

AwsApiGatewayV2Api

El objeto `AwsApiGatewayV2Api` contiene información acerca de una API de versión 2 en Amazon API Gateway.

A continuación, se muestra un ejemplo de resultado de `AwsApiGatewayV2Api` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de `AwsApiGatewayV2Api` los atributos, consulte la [AwsApiGatewayversión 2 ApiDetails en la](#) referencia de la AWS Security Hub API.

Ejemplo

```
"AwsApiGatewayV2Api": {
  "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
  "ApiId": "a1b2c3d4",
  "ApiKeySelectionExpression": "$request.header.x-api-key",
  "CreateDate": "2020-03-28T00:32:37Z",
  "Description": "ApiGatewayV2 Api",
  "Version": "string",
  "Name": "my-api",
  "ProtocolType": "HTTP",
  "RouteSelectionExpression": "$request.method $request.path",
  "CorsConfiguration": {
    "AllowOrigins": [ "*" ],
    "AllowCredentials": true,
    "ExposeHeaders": [ "string" ],
    "MaxAge": 3000,
    "AllowMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowHeaders": [ "*" ]
  }
}
```

AwsApiGatewayV2-Stage

`AwsApiGatewayV2Stage` contiene información sobre una etapa de la versión 2 de Amazon API Gateway.

A continuación, se muestra un ejemplo de resultado de `AwsApiGatewayV2Stage` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de `AwsApiGatewayV2Stage` los atributos, consulte la [AwsApiGatewayversión 2 StageDetails en la](#) referencia de la AWS Security Hub API.

Ejemplo

```
"AwsApiGatewayV2Stage": {
  "CreateDate": "2020-04-08T00:36:05Z",
  "Description": "ApiGatewayV2",
  "DefaultRouteSettings": {
    "DetailedMetricsEnabled": false,
    "LoggingLevel": "INFO",
    "DataTraceEnabled": true,
    "ThrottlingBurstLimit": 100,
    "ThrottlingRateLimit": 50
  },
  "DeploymentId": "x1zwyv",
  "LastUpdatedDate": "2020-04-08T00:36:13Z",
  "RouteSettings": {
    "DetailedMetricsEnabled": false,
    "LoggingLevel": "INFO",
    "DataTraceEnabled": true,
    "ThrottlingBurstLimit": 100,
    "ThrottlingRateLimit": 50
  },
  "StageName": "prod",
  "StageVariables": [
    "function": "my-prod-function"
  ],
  "AccessLogSettings": {
    "Format": "{\"requestId\": \"${context.requestId}\", \"extendedRequestId\": \"${context.extendedRequestId}\", \"ownerAccountId\": \"${context.accountId}\", \"requestAccountId\": \"${context.identity.accountId}\", \"callerPrincipal\": \"${context.identity.caller}\", \"httpMethod\": \"${context.httpMethod}\", \"resourcePath\": \"${context.resourcePath}\", \"status\": \"${context.status}\", \"requestTime\": \"${context.requestTime}\", \"responseLatencyMs\": \"${context.responseLatency}\", \"errorMessage\": \"${context.error.message}\", \"errorResponseType\": \"${context.error.responseType}\", \"apiId\": \"${context.apiId}\", \"awsEndpointRequestId\": \"${context.awsEndpointRequestId}\", \"domainName\": \"${context.domainName}\", \"stage\": \"${context.stage}\", \"xrayTraceId\": \"${context.xrayTraceId}\", \"sourceIp\": \"${context.identity.sourceIp}\", \"user\": \"${context.identity.user}\", \"userAgent\": \"${context.identity.userAgent}\", \"userArn\": \"${context.identity.userArn}\",
```

```

    \"integrationLatency\": \"\${context.integrationLatency}\", \"integrationStatus
\": \"\${context.integrationStatus}\", \"authorizerIntegrationLatency\":
    \"\${context.authorizer.integrationLatency}\" }",
    "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
  },
  "AutoDeploy": false,
  "LastDeploymentStatusMessage": "Message",
  "ApiGatewayManaged": true,
}

```

Recursos de AwsAppSync en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsAppSync los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsAppSyncGraphQLApi

AwsAppSyncGraphQLApi proporciona información sobre una API de AWS AppSync GraphQL, que es una construcción de nivel superior para su aplicación.

En el ejemplo siguiente se muestra el ASFF para el objeto AwsAppSyncGraphQLApi. Para ver las descripciones de los atributos AwsAppSyncGraphQLApi, consulte [AwsAppSyncGraphQLApi](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsAppSyncGraphQLApi": {
  "AdditionalAuthenticationProviders": [
    {
      "AuthenticationType": "AWS_LAMBDA",
      "LambdaAuthorizerConfig": {
        "AuthorizerResultTtlInSeconds": 300,
        "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
      }
    },
    {
      "AuthenticationType": "AWS_IAM"
    }
  ],
}

```

```

    "ApiId": "021345abcdef6789",
    "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
    "AuthenticationType": "API_KEY",
    "Id": "021345abcdef6789",
    "LogConfig": {
      "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-graphqlapi-logs-eu-central-1",
      "ExcludeVerboseContent": true,
      "FieldLogLevel": "ALL"
    },
    "Name": "My AppSync App",
    "XrayEnabled": true,
  }

```

Recursos de AwsAthena en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los AwsAthena recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsAthenaWorkGroup

AwsAthenaWorkGroup proporciona información sobre un grupo de trabajo de Amazon Athena. Un grupo de trabajo le ayuda a separar los usuarios, los equipos, las aplicaciones o las cargas de trabajo. También le ayuda a establecer límites en el procesamiento de datos y a realizar un seguimiento de los costos.

En el ejemplo siguiente se muestra el ASFF para el objeto AwsAthenaWorkGroup. Para ver las descripciones de los atributos AwsAthenaWorkGroup, consulte [AwsAthenaWorkGroup](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsAthenaWorkGroup": {
  "Description": "My workgroup for prod workloads",
  "Name": "MyWorkgroup",
  "WorkgroupConfiguration" {
    "ResultConfiguration": {
      "EncryptionConfiguration": {
        "EncryptionOption": "SSE_KMS",

```

```

        "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
      }
    },
    "State": "ENABLED"
  }

```

Recursos de AwsAutoScaling en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsAutoScaling` los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

`AwsAutoScalingAutoScalingGroup`

El objeto `AwsAutoScalingAutoScalingGroup` proporciona detalles sobre un grupo de escalado automático.

A continuación, se muestra un ejemplo de resultado de `AwsAutoScalingAutoScalingGroup` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsAutoScalingAutoScalingGroup`, consulte [AwsAutoScalingAutoScalingGroupDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsAutoScalingAutoScalingGroup": {
  "CreatedTime": "2017-10-17T14:47:11Z",
  "HealthCheckGracePeriod": 300,
  "HealthCheckType": "EC2",
  "LaunchConfigurationName": "mylaunchconf",
  "LoadBalancerNames": [],
  "LaunchTemplate": {
    "LaunchTemplateId": "string",
    "LaunchTemplateName": "string",
    "Version": "string"
  },
  "MixedInstancesPolicy": {
    "InstancesDistribution": {
      "OnDemandAllocationStrategy": "prioritized",

```

```

        "OnDemandBaseCapacity": number,
        "OnDemandPercentageAboveBaseCapacity": number,
        "SpotAllocationStrategy": "lowest-price",
        "SpotInstancePools": number,
        "SpotMaxPrice": "string"
    },
    "LaunchTemplate": {
        "LaunchTemplateSpecification": {
            "LaunchTemplateId": "string",
            "LaunchTemplateName": "string",
            "Version": "string"
        },
        "CapacityRebalance": true,
        "Overrides": [
            {
                "InstanceType": "string",
                "WeightedCapacity": "string"
            }
        ]
    }
}

```

AwsAutoScalingLaunchConfiguration

El objeto `AwsAutoScalingLaunchConfiguration` proporciona detalles sobre la configuración de una característica de .

A continuación se muestra un ejemplo de `AwsAutoScalingLaunchConfiguration` búsqueda en el formato AWS de búsqueda de seguridad (ASFF).

Para ver las descripciones de los atributos `AwsAutoScalingLaunchConfiguration`, consulte [AwsAutoScalingLaunchConfigurationDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

AwsAutoScalingLaunchConfiguration: {
    "LaunchConfigurationName": "newtest",
    "ImageId": "ami-058a3739b02263842",
    "KeyName": "55hundredinstance",
    "SecurityGroups": [ "sg-01fce87ad6e019725" ],
    "ClassicLinkVpcSecurityGroups": [],

```

```
"UserData": "...Base64-Encoded user data..."
"InstanceType": "a1.metal",
"KernelId": "",
"RamdiskId": "ari-a51cf9cc",
"BlockDeviceMappings": [
  {
    "DeviceName": "/dev/sdh",
    "Ebs": {
      "VolumeSize": 30,
      "VolumeType": "gp2",
      "DeleteOnTermination": false,
      "Encrypted": true,
      "SnapshotId": "snap-ffaa1e69",
      "VirtualName": "ephemeral1"
    }
  },
  {
    "DeviceName": "/dev/sdb",
    "NoDevice": true
  },
  {
    "DeviceName": "/dev/sda1",
    "Ebs": {
      "SnapshotId": "snap-02420cd3d2dea1bc0",
      "VolumeSize": 8,
      "VolumeType": "gp2",
      "DeleteOnTermination": true,
      "Encrypted": false
    }
  },
  {
    "DeviceName": "/dev/sdi",
    "Ebs": {
      "VolumeSize": 20,
      "VolumeType": "gp2",
      "DeleteOnTermination": false,
      "Encrypted": true
    }
  },
  {
    "DeviceName": "/dev/sdc",
    "NoDevice": true
  }
],
```

```
"InstanceMonitoring": {
  "Enabled": false
},
"CreatedTime": 1620842933453,
"EbsOptimized": false,
"AssociatePublicIpAddress": true,
"SpotPrice": "0.045"
}
```

Recursos de AwsBackup en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsBackup los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsBackupBackupPlan

El objeto AwsBackupBackupPlan proporciona información sobre un proyecto de plan de copia de seguridad de AWS Backup . Un plan AWS Backup de respaldo es una expresión de política que define cuándo y cómo desea hacer una copia de seguridad de sus AWS recursos.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del AwsBackupBackupPlan objeto. Para ver las descripciones de los atributos AwsBackupBackupPlan, consulte [AwsBackupBackupPlan](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsBackupBackupPlan": {
  "BackupPlan": {
    "AdvancedBackupSettings": [{
      "BackupOptions": {
        "WindowsVSS": "enabled"
      },
      "ResourceType": "EC2"
    }],
    "BackupPlanName": "test",
    "BackupPlanRule": [{
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
```

```

    "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
    "Lifecycle": {
      "DeleteAfterDays": 365,
      "MoveToColdStorageAfterDays": 30
    }
  ]],
  "Lifecycle": {
    "DeleteAfterDays": 35
  },
  "RuleName": "DailyBackups",
  "ScheduleExpression": "cron(0 5 ? * * *)",
  "StartWindowMinutes": 480,
  "TargetBackupVault": "Default"
},
{
  "CompletionWindowMinutes": 10080,
  "CopyActions": [{
    "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
    "Lifecycle": {
      "DeleteAfterDays": 365,
      "MoveToColdStorageAfterDays": 30
    }
  ]],
  "Lifecycle": {
    "DeleteAfterDays": 35
  },
  "RuleName": "Monthly",
  "ScheduleExpression": "cron(0 5 1 * ? *)",
  "StartWindowMinutes": 480,
  "TargetBackupVault": "Default"
}]
},
"BackupPlanArn": "arn:aws:backup:us-east-1:858726136373:backup-
plan:b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
"BackupPlanId": "b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
"VersionId": "ZDVjNDIzMjItYTZiNS00NzczLTg4YzctNmExMWM2NjZhY2E1"
}

```


AwsBackupBackupVault

El objeto `AwsBackupBackupVault` proporciona información sobre un almacén de copias de seguridad de AWS Backup . Una bóveda AWS Backup de copias de seguridad es un contenedor que almacena y organiza las copias de seguridad.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsBackupBackupVault` objeto. Para ver las descripciones de los atributos `AwsBackupBackupVault`, consulte [AwsBackupBackupVault](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsBackupBackupVault": {
  "AccessPolicy": {
    "Statement": [{
      "Action": [
        "backup:DeleteBackupVault",
        "backup:DeleteBackupVaultAccessPolicy",
        "backup:DeleteRecoveryPoint",
        "backup:StartCopyJob",
        "backup:StartRestoreJob",
        "backup:UpdateRecoveryPointLifecycle"
      ],
      "Effect": "Deny",
      "Principal": {
        "AWS": "*"
      },
      "Resource": "*"
    }],
    "Version": "2012-10-17"
  },
  "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/automatic-backup-vault",
  "BackupVaultName": "aws/efs/automatic-backup-vault",
  "EncryptionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-ba38-838bf8d06ca0",
  "Notifications": {
    "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED", "COPY_JOB_STARTED"],
    "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
  }
}
```

}

AwsBackupRecoveryPoint

El objeto `AwsBackupRecoveryPoint` proporciona información sobre una copia de seguridad de AWS Backup, también denominada punto de recuperación. Un punto de AWS Backup recuperación representa el contenido de un recurso en un momento específico.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsBackupRecoveryPoint` objeto. Para ver las descripciones de los atributos `AwsBackupRecoveryPoint`, consulte [AwsBackupRecoveryPoint](#) en la referencia de la API de AWS Security Hub.

Ejemplo

```
"AwsBackupRecoveryPoint": {
  "BackupSizeInBytes": 0,
  "BackupVaultName": "aws/efs/automatic-backup-vault",
  "BackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/automatic-backup-vault",
  "CalculatedLifecycle": {
    "DeleteAt": "2021-08-30T06:51:58.271Z",
    "MoveToColdStorageAt": "2020-08-10T06:51:58.271Z"
  },
  "CompletionDate": "2021-07-26T07:21:40.361Z",
  "CreatedBy": {
    "BackupPlanArn": "arn:aws:backup:us-east-1:111122223333:backup-plan:aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
    "BackupPlanId": "aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
    "BackupPlanVersion": "ZGM4YzY5YjktMWYxNC00ZTBmLWE5MjYtZmU5OWNiZmM5ZjIz",
    "BackupRuleId": "2a600c2-42ad-4196-808e-084923ebfd25"
  },
  "CreationDate": "2021-07-26T06:51:58.271Z",
  "EncryptionKeyArn": "arn:aws:kms:us-east-1:111122223333:key/72ba68d4-5e43-40b0-ba38-838bf8d06ca0",
  "IamRoleArn": "arn:aws:iam::111122223333:role/aws-service-role/backup.amazonaws.com/AWSServiceRoleForBackup",
  "IsEncrypted": true,
  "LastRestoreTime": "2021-07-26T06:51:58.271Z",
  "Lifecycle": {
    "DeleteAfterDays": 35,
    "MoveToColdStorageAfterDays": 15
  },
}
```

```

    "RecoveryPointArn": "arn:aws:backup:us-east-1:111122223333:recovery-point:151a59e4-
f1d5-4587-a7fd-0774c6e91268",
    "ResourceArn": "arn:aws:elasticfilesystem:us-east-1:858726136373:file-system/
fs-15bd31a1",
    "ResourceType": "EFS",
    "SourceBackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/
efs/automatic-backup-vault",
    "Status": "COMPLETED",
    "StatusMessage": "Failure message",
    "StorageClass": "WARM"
}

```

Recursos de AwsCertificateManager en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los AwsCertificateManager recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsCertificateManagerCertificate

El objeto AwsCertificateManagerCertificate proporciona detalles sobre un certificado de AWS Certificate Manager (ACM).

A continuación se muestra un ejemplo de AwsCertificateManagerCertificate búsqueda en el formato AWS de búsqueda de seguridad (ASFF). Para ver las descripciones de los atributos AwsCertificateManagerCertificate, consulte [AwsCertificateManagerCertificateDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsCertificateManagerCertificate": {
    "CertificateAuthorityArn": "arn:aws:acm:us-west-2:444455556666:certificate-
authority/example",
    "CreatedAt": "2019-05-24T18:12:02.000Z",
    "DomainName": "example.amazondomains.com",
    "DomainValidationOptions": [
        {
            "DomainName": "example.amazondomains.com",
            "ResourceRecord": {
                "Name": "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                "Type": "CNAME",

```

```

        "Value": "_example.acm-validations.aws."
      },
      "ValidationDomain": "example.amazondomains.com",
      "ValidationEmails": [sample_email@sample.com],
      "ValidationMethod": "DNS",
      "ValidationStatus": "SUCCESS"
    }
  ],
  "ExtendedKeyUsages": [
    {
      "Name": "TLS_WEB_SERVER_AUTHENTICATION",
      "OId": "1.3.6.1.5.5.7.3.1"
    },
    {
      "Name": "TLS_WEB_CLIENT_AUTHENTICATION",
      "OId": "1.3.6.1.5.5.7.3.2"
    }
  ],
  "FailureReason": "",
  "ImportedAt": "2018-08-17T00:13:00.000Z",
  "InUseBy": ["arn:aws:amazondomains:us-west-2:444455556666:loadbalancer/example"],
  "IssuedAt": "2020-04-26T00:41:17.000Z",
  "Issuer": "Amazon",
  "KeyAlgorithm": "RSA-1024",
  "KeyUsages": [
    {
      "Name": "DIGITAL_SIGNATURE",
    },
    {
      "Name": "KEY_ENCIPHERMENT",
    }
  ],
  "NotAfter": "2021-05-26T12:00:00.000Z",
  "NotBefore": "2020-04-26T00:00:00.000Z",
  "Options": {
    "CertificateTransparencyLoggingPreference": "ENABLED",
  }
  "RenewalEligibility": "ELIGIBLE",
  "RenewalSummary": {
    "DomainValidationOptions": [
      {
        "DomainName": "example.amazondomains.com",
        "ResourceRecord": {

```

```

        "Name":
"_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
        "Type": "CNAME",
        "Value": "_example.acm-validations.aws.com",
    },
    "ValidationDomain": "example.amazondomains.com",
    "ValidationEmails": ["sample_email@sample.com"],
    "ValidationMethod": "DNS",
    "ValidationStatus": "SUCCESS"
}
],
"RenewalStatus": "SUCCESS",
"RenewalStatusReason": "",
"UpdatedAt": "2020-04-26T00:41:35.000Z",
},
"Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
"SignatureAlgorithm": "SHA256WITHRSA",
"Status": "ISSUED",
"Subject": "CN=example.amazondomains.com",
"SubjectAlternativeNames": ["example.amazondomains.com"],
"Type": "AMAZON_ISSUED"
}

```

Recursos de AwsCloudFormation en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsCloudFormation los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsCloudFormationStack

El objeto AwsCloudFormationStack proporciona detalles acerca de una pila de AWS CloudFormation que está anidada como un recurso en una plantilla de nivel superior.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del AwsCloudFormationStack objeto. Para ver las descripciones de los atributos AwsCloudFormationStack, consulte [AwsCloudFormationStackDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsCloudFormationStack": {
  "Capabilities": [
    "CAPABILITY_IAM",
    "CAPABILITY_NAMED_IAM"
  ],
  "CreationTime": "2022-02-18T15:31:53.161Z",
  "Description": "AWS CloudFormation Sample",
  "DisableRollback": true,
  "DriftInformation": {
    "StackDriftStatus": "DRIFTED"
  },
  "EnableTerminationProtection": false,
  "LastUpdatedTime": "2022-02-18T15:31:53.161Z",
  "NotificationArns": [
    "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
  ],
  "Outputs": [{
    "Description": "URL for newly created LAMP stack",
    "OutputKey": "WebsiteUrl",
    "OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
  }],
  "RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
  "StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
  "StackName": "sample-stack",
  "StackStatus": "CREATE_COMPLETE",
  "StackStatusReason": "Success",
  "TimeoutInMinutes": 1
}

```

Recursos de AwsCloudFront en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsCloudFront los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsCloudFrontDistribution

El `AwsCloudFrontDistribution` objeto proporciona detalles sobre una configuración de CloudFront distribución de Amazon.

A continuación, se muestra un ejemplo de resultado de `AwsCloudFrontDistribution` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsCloudFrontDistribution`, consulte [AwsCloudFrontDistributionDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsCloudFrontDistribution": {
  "CacheBehaviors": {
    "Items": [
      {
        "ViewerProtocolPolicy": "https-only"
      }
    ]
  },
  "DefaultCacheBehavior": {
    "ViewerProtocolPolicy": "https-only"
  },
  "DefaultRootObject": "index.html",
  "DomainName": "d2wkuj2w9l34gt.cloudfront.net",
  "Etag": "E37H0T42DHPVYH",
  "LastModifiedTime": "2015-08-31T21:11:29.093Z",
  "Logging": {
    "Bucket": "myawslogbucket.s3.amazonaws.com",
    "Enabled": false,
    "IncludeCookies": false,
    "Prefix": "myawslog/"
  },
  "OriginGroups": {
    "Items": [
      {
        "FailoverCriteria": {
          "StatusCodes": {
            "Items": [
              200,
              301,
              404
            ]
          }
        },
        "Quantity": 3
      }
    ]
  }
}
```

```

    },
    "Origins": {
      "Items": [
        {
          "CustomOriginConfig": {
            "HttpPort": 80,
            "HttpsPort": 443,
            "OriginKeepaliveTimeout": 60,
            "OriginProtocolPolicy": "match-viewer",
            "OriginReadTimeout": 30,
            "OriginSslProtocols": {
              "Items": ["SSLv3", "TLSv1"],
              "Quantity": 2
            }
          },
          "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
          "Id": "my-origin",
          "OriginPath": "/production",
          "S3OriginConfig": {
            "OriginAccessIdentity": "origin-access-identity/cloudfront/
E2YFS67H6VB6E4"
          }
        }
      ],
      "Status": "Deployed",
      "ViewerCertificate": {
        "AcmCertificateArn": "arn:aws:acm::123456789012:AcmCertificateArn",
        "Certificate": "ASCAJRRE5XYF52TKRY5M4",
        "CertificateSource": "iam",
        "CloudFrontDefaultCertificate": true,
        "IamCertificateId": "ASCAJRRE5XYF52TKRY5M4",
        "MinimumProtocolVersion": "TLSv1.2_2021",
        "SslSupportMethod": "sni-only"
      },
      "WebAclId": "waf-1234567890"
    }
  }
}

```


Recursos de AwsCloudTrail en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsCloudTrail` los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

`AwsCloudTrailTrail`

El objeto `AwsCloudTrailTrail` proporciona detalles sobre un seguimiento de AWS CloudTrail .

A continuación, se muestra un ejemplo de resultado de `AwsCloudTrailTrail` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsCloudTrailTrail`, consulte [AwsCloudTrailTrailDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsCloudTrailTrail": {
  "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:CloudTrail/regression:*",
  "CloudWatchLogsRoleArn": "arn:aws:iam::866482105055:role/
CloudTrail_CloudWatchLogs",
  "HasCustomEventSelectors": true,
  "HomeRegion": "us-west-2",
  "IncludeGlobalServiceEvents": true,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": false,
  "KmsKeyId": "kmsKeyId",
  "LogFileValidationEnabled": true,
  "Name": "regression-trail",
  "S3BucketName": "cloudtrail-bucket",
  "S3KeyPrefix": "s3KeyPrefix",
  "SnsTopicArn": "arn:aws:sns:us-east-2:123456789012:MyTopic",
  "SnsTopicName": "snsTopicName",
  "TrailArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail"
}
```

Recursos de AwsCloudWatch en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsCloudWatch` los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsCloudWatchAlarm

El `AwsCloudWatchAlarm` objeto proporciona detalles sobre CloudWatch las alarmas de Amazon que vigilan una métrica o realizan una acción cuando una alarma cambia de estado.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsCloudWatchAlarm` objeto. Para ver las descripciones de los atributos `AwsCloudWatchAlarm`, consulte [AwsCloudWatchAlarmDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsCloudWatchAlarm": {
  "ActionsEnabled": true,
  "AlarmActions": [
    "arn:aws:automate:region:ec2:stop",
    "arn:aws:automate:region:ec2:terminate"
  ],
  "AlarmArn": "arn:aws:cloudwatch:us-west-2:012345678910:alarm:sampleAlarm",
  "AlarmConfigurationUpdatedTimestamp": "2022-02-18T15:31:53.161Z",
  "AlarmDescription": "Alarm Example",
  "AlarmName": "Example",
  "ComparisonOperator": "GreaterThanOrEqualToThreshold",
  "DatapointsToAlarm": 1,
  "Dimensions": [{
    "Name": "InstanceId",
    "Value": "i-1234567890abcdef0"
  }],
  "EvaluateLowSampleCountPercentile": "evaluate",
  "EvaluationPeriods": 1,
  "ExtendedStatistic": "p99.9",
  "InsufficientDataActions": [
    "arn:aws:automate:region:ec2:stop"
  ],
  "MetricName": "Sample Metric",
  "Namespace": "YourNamespace",
  "OkActions": [
    "arn:aws:swf:region:account-id:action/actions/AWS_EC2.InstanceId.Stop/1.0"
  ],
  "Period": 1,
  "Statistic": "SampleCount",
```

```
"Threshold": 12.3,
"ThresholdMetricId": "t1",
"TreatMissingData": "notBreaching",
"Unit": "Kilobytes/Second"
}
```

Recursos de AwsCodeBuild en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsCodeBuild los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsCodeBuildProject

El objeto `AwsCodeBuildProject` proporciona información sobre un proyecto de AWS CodeBuild .

A continuación, se muestra un ejemplo de resultado de `AwsCodeBuildProject` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsCodeBuildProject`, consulte [AwsCodeBuildProjectDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsCodeBuildProject": {
  "Artifacts": [
    {
      "ArtifactIdentifier": "string",
      "EncryptionDisabled": boolean,
      "Location": "string",
      "Name": "string",
      "NamespaceType": "string",
      "OverrideArtifactName": boolean,
      "Packaging": "string",
      "Path": "string",
      "Type": "string"
    }
  ],
  "SecondaryArtifacts": [
    {
      "ArtifactIdentifier": "string",
      "EncryptionDisabled": boolean,
```

```

        "Location": "string",
        "Name": "string",
        "NamespaceType": "string",
        "OverrideArtifactName": boolean,
        "Packaging": "string",
        "Path": "string",
        "Type": "string"
    }
],
"EncryptionKey": "string",
"Certificate": "string",
"Environment": {
    "Certificate": "string",
    "EnvironmentVariables": [
        {
            "Name": "string",
            "Type": "string",
            "Value": "string"
        }
    ]
},
"ImagePullCredentialsType": "string",
"PrivilegedMode": boolean,
"RegistryCredential": {
    "Credential": "string",
    "CredentialProvider": "string"
},
"Type": "string"
},
"LogsConfig": {
    "CloudWatchLogs": {
        "GroupName": "string",
        "Status": "string",
        "StreamName": "string"
    },
    "S3Logs": {
        "EncryptionDisabled": boolean,
        "Location": "string",
        "Status": "string"
    }
},
"Name": "string",
"ServiceRole": "string",
"Source": {
    "Type": "string",

```

```

        "Location": "string",
        "GitCloneDepth": integer
    },
    "VpcConfig": {
        "VpcId": "string",
        "Subnets": ["string"],
        "SecurityGroupIds": ["string"]
    }
}

```

Recursos de AwsDms en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsDms los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsDmsEndpoint

El `AwsDmsEndpoint` objeto proporciona información sobre un punto final AWS Database Migration Service (AWS DMS). Un punto de conexión proporciona información de conexión, tipo de almacén de datos y ubicación acerca de su almacén de datos.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsDmsEndpoint` objeto. Para ver las descripciones de los atributos `AwsDmsEndpoint`, consulte [AwsDmsEndpointDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsDmsEndpoint": {
    "CertificateArn": "arn:aws:dms:us-east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWFI",
    "DatabaseName": "Test",
    "EndpointArn": "arn:aws:dms:us-east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBPNK6MJQVQVQA",
    "EndpointIdentifier": "target-db",
    "EndpointType": "TARGET",
    "EngineName": "mariadb",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
}

```

```
"Port": 3306,  
"ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",  
"SslMode": "verify-ca",  
"Username": "admin"  
}
```

AwsDmsReplicationInstance

El `AwsDmsReplicationInstance` objeto proporciona información sobre una instancia de replicación AWS Database Migration Service (AWS DMS). DMS utiliza una instancia de replicación para conectarse con su almacén de datos de origen, leer los datos de origen y formatear los datos para que el almacén de datos de destino pueda consumirlos.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsDmsReplicationInstance` objeto. Para ver las descripciones de los atributos `AwsDmsReplicationInstance`, consulte [AwsDmsReplicationInstanceDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsDmsReplicationInstance": {  
  "AllocatedStorage": 50,  
  "AutoMinorVersionUpgrade": true,  
  "AvailabilityZone": "us-east-1b",  
  "EngineVersion": "3.5.1",  
  "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-  
EXAMPLE11111",  
  "MultiAZ": false,  
  "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",  
  "PubliclyAccessible": true,  
  "ReplicationInstanceClass": "dms.c5.xlarge",  
  "ReplicationInstanceIdentifier": "second-replication-instance",  
  "ReplicationSubnetGroup": {  
    "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"  
  },  
  "VpcSecurityGroups": [  
    {  
      "VpcSecurityGroupId": "sg-003a34e205138138b"  
    }  
  ]  
}
```

AwsDmsReplicationTask

El `AwsDmsReplicationTask` objeto proporciona información sobre una tarea de replicación AWS Database Migration Service (AWS DMS). Una tarea de replicación mueve un conjunto de datos desde el punto de conexión de origen al punto de conexión de destino.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsDmsReplicationInstance` objeto. Para ver las descripciones de los atributos `AwsDmsReplicationInstance`, consulte [AwsDmsReplicationInstance](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsDmsReplicationTask": {
  "CdcStartPosition": "2023-08-28T14:26:22",
  "Id": "arn:aws:dms:us-east-1:123456789012:task:YDYU0HZIXWKQSUCBMUCQCN44SJW74VJNB5DFWQ",
  "MigrationType": "cdc",
  "ReplicationInstanceArn": "arn:aws:dms:us-east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4YOUGIMYJUI",
  "ReplicationTaskIdentifier": "test-task",
  "ReplicationTaskSettings": "{\n\"Logging\":{\n\"EnableLogging\":false,\n\"EnableLogContext\":false,\n\"LogComponents\":[\n{\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"TRANSFORMATION\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"SOURCE_UNLOAD\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"IO\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"TARGET_LOAD\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"PERFORMANCE\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"SOURCE_CAPTURE\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"SORTER\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"REST_SERVER\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"VALIDATOR_EXT\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"TARGET_APPLY\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"TASK_MANAGER\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"TABLES_MANAGER\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"METADATA_MANAGER\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"FILE_FACTORY\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"COMMON\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"ADDONS\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"DATA_STRUCTURE\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"COMMUNICATION\n\"}, {\n\"Severity\":\n\"LOGGER_SEVERITY_DEFAULT\n\", \n\"Id\":\n\"FILE_TRANSFER\n\"}]\n,\"CloudWatchLogGroup\n\":null,\n\"CloudWatchLogStream\n\":null},\n\"StreamBufferSettings\":{\n\"StreamBufferCount\n\":3,\n\"CtrlStreamBufferSizeInMB\n\":5,\n\"StreamBufferSizeInMB\n\":8},\n\"ErrorBehavior\n\":{\n\"FailOnNoTablesCaptured\n\":true,\n\"ApplyErrorUpdatePolicy\n\":\n\"LOG_ERROR\n\", \n\"FailOnTransactionConsistencyBreached\n\":false,\n\"RecoverableErrorThrottlingMax\n\":1800,
```

```

\ "DataErrorEscalationPolicy\":\ "SUSPEND_TABLE\","ApplyErrorEscalationCount\":0,
\ "RecoverableErrorStopRetryAfterThrottlingMax\":true,\ "RecoverableErrorThrottling
\":true,\ "ApplyErrorFailOnTruncationDdl\":false,\ "DataTruncationErrorPolicy\":
\ "LOG_ERROR\","ApplyErrorInsertPolicy\":\ "LOG_ERROR\","EventErrorPolicy\":
\ "IGNORE\","ApplyErrorEscalationPolicy\":\ "LOG_ERROR\","RecoverableErrorCount
\":-1,\ "DataErrorEscalationCount\":0,\ "TableErrorEscalationPolicy\":\ "STOP_TASK
\","RecoverableErrorInterval\":5,\ "ApplyErrorDeletePolicy\":\ "IGNORE_RECORD\","
\ "TableErrorEscalationCount\":0,\ "FullLoadIgnoreConflicts\":true,\ "DataErrorPolicy
\":\ "LOG_ERROR\","TableErrorPolicy\":\ "SUSPEND_TABLE\"},"TTSettings
\":{\ "TTS3Settings\":null,\ "TTRecordSettings\":null,\ "EnableTT\":false},
\ "FullLoadSettings\":{\ "CommitRate\":10000,\ "StopTaskCachedChangesApplied
\":false,\ "StopTaskCachedChangesNotApplied\":false,\ "MaxFullLoadSubTasks
\":8,\ "TransactionConsistencyTimeout\":600,\ "CreatePkAfterFullLoad\":false,
\ "TargetTablePrepMode\":\ "DO_NOTHING\"},"TargetMetadata\":{\ "ParallelApplyBufferSize
\":0,\ "ParallelApplyQueuesPerThread\":0,\ "ParallelApplyThreads\":0,\ "TargetSchema
\":\ "",\ "InlineLobMaxSize\":0,\ "ParallelLoadQueuesPerThread\":0,\ "SupportLobs
\":true,\ "LobChunkSize\":64,\ "TaskRecoveryTableEnabled\":false,\ "ParallelLoadThreads
\":0,\ "LobMaxSize\":0,\ "BatchApplyEnabled\":false,\ "FullLobMode\":true,
\ "LimitedSizeLobMode\":false,\ "LoadMaxFileSize\":0,\ "ParallelLoadBufferSize\":0},
\ "BeforeImageSettings\":null,\ "ControlTablesSettings\":{\ "historyTimeslotInMinutes
\":5,\ "HistoryTimeslotInMinutes\":5,\ "StatusTableEnabled\":false,
\ "SuspendedTablesTableEnabled\":false,\ "HistoryTableEnabled\":false,\ "ControlSchema
\":\ "",\ "FullLoadExceptionTableEnabled\":false},\ "LoopbackPreventionSettings
\":null,\ "CharacterSetSettings\":null,\ "FailTaskWhenCleanTaskResourceFailed
\":false,\ "ChangeProcessingTuning\":{\ "StatementCacheSize\":50,\ "CommitTimeout
\":1,\ "BatchApplyPreserveTransaction\":true,\ "BatchApplyTimeoutMin\":1,
\ "BatchSplitSize\":0,\ "BatchApplyTimeoutMax\":30,\ "MinTransactionSize\":1000,
\ "MemoryKeepTime\":60,\ "BatchApplyMemoryLimit\":500,\ "MemoryLimitTotal\":1024},
\ "ChangeProcessingDdlHandlingPolicy\":{\ "HandleSourceTableDropped\":true,
\ "HandleSourceTableTruncated\":true,\ "HandleSourceTableAltered\":true},
\ "PostProcessingRules\":null}],
  "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHYOKVKRNHAKJ4Q3RUXACNGFGYWRI",
  "TableMappings": "{\ "rules\":[{\ "rule-type\":\ "selection\","rule-id\":
\ "969761702\","rule-name\":\ "969761702\","object-locator\":{\ "schema-name\":\ "%table
\","table-name\":\ "%example\"},"rule-action\":\ "exclude\","filters\":[ ]}]}",
  "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:ABR8LB0QB3CZY33F7XV253NAJBPNPK6MJQVQVQA"
}

```


Recursos de AwsDynamoDB en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los recursos. AwsDynamoDB

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsDynamoDbTable

El objeto `AwsDynamoDbTable` proporciona detalles sobre una tabla de Amazon DynamoDB.

A continuación, se muestra un ejemplo de resultado de `AwsDynamoDbTable` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsDynamoDbTable`, consulte [AwsDynamoDbTableDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsDynamoDbTable": {
  "AttributeDefinitions": [
    {
      "AttributeName": "attribute1",
      "AttributeType": "value 1"
    },
    {
      "AttributeName": "attribute2",
      "AttributeType": "value 2"
    },
    {
      "AttributeName": "attribute3",
      "AttributeType": "value 3"
    }
  ],
  "BillingModeSummary": {
    "BillingMode": "PAY_PER_REQUEST",
    "LastUpdateToPayPerRequestDateTime": "2019-12-03T15:23:10.323Z"
  },
  "CreationDateTime": "2019-12-03T15:23:10.248Z",
  "DeletionProtectionEnabled": true,
  "GlobalSecondaryIndexes": [
    {
      "Backfilling": false,
```

```

        "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
index/exampleIndex",
        "IndexName": "standardsControlArnIndex",
        "IndexSizeBytes": 1862513,
        "IndexStatus": "ACTIVE",
        "ItemCount": 20,
        "KeySchema": [
            {
                "AttributeName": "City",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "Date",
                "KeyType": "RANGE"
            }
        ],
        "Projection": {
            "NonKeyAttributes": ["predictorName"],
            "ProjectionType": "ALL"
        },
        "ProvisionedThroughput": {
            "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
            "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
            "NumberOfDecreasesToday": 0,
            "ReadCapacityUnits": 100,
            "WriteCapacityUnits": 50
        },
    },
],
"GlobalTableVersion": "V1",
"ItemCount": 2705,
"KeySchema": [
    {
        "AttributeName": "zipcode",
        "KeyType": "HASH"
    }
],
"LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
"LatestStreamLabel": "2019-12-03T23:23:10.248",
"LocalSecondaryIndexes": [
    {
        "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",

```

```

        "IndexName": "CITY_DATE_INDEX_NAME",
        "KeySchema": [
            {
                "AttributeName": "zipcode",
                "KeyType": "HASH"
            }
        ],
        "Projection": {
            "NonKeyAttributes": ["predictorName"],
            "ProjectionType": "ALL"
        },
    },
],
"ProvisionedThroughput": {
    "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
    "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
    "NumberOfDecreasesToday": 0,
    "ReadCapacityUnits": 100,
    "WriteCapacityUnits": 50
},
"Replicas": [
    {
        "GlobalSecondaryIndexes": [
            {
                "IndexName": "CITY_DATE_INDEX_NAME",
                "ProvisionedThroughputOverride": {
                    "ReadCapacityUnits": 10
                }
            }
        ],
        "KmsMasterKeyId": "KmsKeyId",
        "ProvisionedThroughputOverride": {
            "ReadCapacityUnits": 10
        },
        "RegionName": "regionName",
        "ReplicaStatus": "CREATING",
        "ReplicaStatusDescription": "replicaStatusDescription"
    }
],
"RestoreSummary": {
    "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/backup/backup1",
    "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
    "RestoreDateTime": "2020-06-22T17:40:12.322Z",

```

```

    "RestoreInProgress": true
  },
  "SseDescription": {
    "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
    "Status": "ENABLED",
    "SseType": "KMS",
    "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
  },
  "StreamSpecification" : {
    "StreamEnabled": true,
    "StreamViewType": "NEW_IMAGE"
  },
  "TableId": "example-table-id-1",
  "TableName": "example-table",
  "TableSizeBytes": 1862513,
  "TableStatus": "ACTIVE"
}

```

Recursos de AwsEc2 en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsEc2 los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsEc2ClientVpnEndpoint

El `AwsEc2ClientVpnEndpoint` objeto proporciona información sobre un AWS Client VPN punto final. El punto de conexión de Client VPN es el recurso que crea y configura para habilitar y administrar sesiones de Client VPN. Es el punto de terminación de todas las sesiones de Client VPN.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsEc2ClientVpnEndpoint` objeto. Para ver las descripciones de `AwsEc2ClientVpnEndpoint` los atributos, consulta el apartado [AwsEc2](#) de `ClientVpnEndpointDetails` la referencia de la AWS Security Hub API.

Ejemplo

```

"AwsEc2ClientVpnEndpoint": {
  "AuthenticationOptions": [
    {

```

```

      "MutualAuthentication": {
        "ClientRootCertificateChainArn": "arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      },
      "Type": "certificate-authentication"
    }
  ],
  "ClientCidrBlock": "10.0.0.0/22",
  "ClientConnectOptions": {
    "Enabled": false
  },
  "ClientLoginBannerOptions": {
    "Enabled": false
  },
  "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
  "ConnectionLogOptions": {
    "Enabled": false
  },
  "Description": "test",
  "DnsServer": ["10.0.0.0"],
  "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "SecurityGroupIdSet": [
    "sg-0f7a177b82b443691"
  ],
  "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/
cvpn-endpoint-00c5d11fc4729f2a5",
  "SessionTimeoutHours": 24,
  "SplitTunnel": false,
  "TransportProtocol": "udp",
  "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
  "VpnPort": 443
}

```

AwsEc2Eip

El objeto `AwsEc2Eip` proporciona información sobre una dirección IP elástica.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsEc2Eip` objeto. Para ver las descripciones de `AwsEc2Eip` los atributos, consulta el apartado [AwsEc2](#) de `EipDetails` la referencia de la AWS Security Hub API.

Ejemplo

```
"AwsEc2Eip": {
  "InstanceId": "instance1",
  "PublicIp": "192.0.2.04",
  "AllocationId": "eipalloc-example-id-1",
  "AssociationId": "eipassoc-example-id-1",
  "Domain": "vpc",
  "PublicIpv4Pool": "anycompany",
  "NetworkBorderGroup": "eu-central-1",
  "NetworkInterfaceId": "eni-example-id-1",
  "NetworkInterfaceOwnerId": "777788889999",
  "PrivateIpAddress": "192.0.2.03"
}
```

AwsEc2Instance

El `AwsEc2Instance` objeto proporciona detalles sobre una EC2 instancia de Amazon.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsEc2Instance` objeto. Para ver las descripciones de `AwsEc2Instance` los atributos, consulta el apartado [AwsEc2](#) de InstanceDetails la referencia de la AWS Security Hub API.

Ejemplo

```
"AwsEc2Instance": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
  "ImageId": "ami-1234",
  "IPv4Addresses": [ "1.1.1.1" ],
  "IPv6Addresses": [ "2001:db8:1234:1a2b::123" ],
  "KeyName": "my_keypair",
  "LaunchedAt": "2018-05-08T16:46:19.000Z",
  "MetadataOptions": {
    "HttpEndpoint": "enabled",
    "HttpProtocolIpv6": "enabled",
    "HttpPutResponseHopLimit": 1,
    "HttpTokens": "optional",
    "InstanceMetadataTags": "disabled",
  },
  "Monitoring": {
    "State": "disabled"
  },
  "NetworkInterfaces": [
    {
```

```

        "NetworkInterfaceId": "eni-e5aa89a3"
    }
],
"SubnetId": "subnet-123",
"Type": "i3.xlarge",
"VpcId": "vpc-123"
}

```

AwsEc2LaunchTemplate

El objeto `AwsEc2LaunchTemplate` contiene detalles sobre una plantilla de lanzamiento de Amazon Elastic Compute Cloud que especifica la información de configuración de la instancia.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsEc2LaunchTemplate` objeto. Para ver las descripciones de `AwsEc2LaunchTemplate` los atributos, consulta el apartado [AwsEc2](#) de `LaunchTemplateDetails` la referencia de la AWS Security Hub API.

Ejemplo

```

"AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "1",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "lt-0a16e9802800bdd85",
    "ImageId": "ami-0d5eff06f840b45e9",
    "LatestVersionNumber": "1",
    "LaunchTemplateData": {
        "BlockDeviceMappings": [{
            "DeviceName": "/dev/xvda",
            "Ebs": {
                "DeleteonTermination": true,
                "Encrypted": true,
                "SnapshotId": "snap-01047646ec075f543",
                "VolumeSize": 8,
                "VolumeType": "gp2"
            }
        }],
        "MetadataOptions": {
            "HttpTokens": "enabled",
            "HttpPutResponseHopLimit": 1
        },
        "Monitoring": {

```

```
    "Enabled": true,
    "NetworkInterfaces": [{
      "AssociatePublicIpAddress" : true,
    }],
    "LaunchTemplateName": "string",
    "LicenseSpecifications": ["string"],
    "SecurityGroupIds": ["sg-01fce87ad6e019725"],
    "SecurityGroups": ["string"],
    "TagSpecifications": ["string"]
  }
```

AwsEc2NetworkAcl

El `AwsEc2NetworkAcl` objeto contiene detalles sobre una lista de control de acceso (ACL) a la EC2 red de Amazon.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2NetworkAcl` objeto. Para ver las descripciones de `AwsEc2NetworkAcl` los atributos, consulta el apartado [AwsEc2](#) de `NetworkAclDetails` la referencia de la AWS Security Hub API.

Ejemplo

```
"AwsEc2NetworkAcl": {
  "IsDefault": false,
  "NetworkAclId": "acl-1234567890abcdef0",
  "OwnerId": "123456789012",
  "VpcId": "vpc-1234abcd",
  "Associations": [{
    "NetworkAclAssociationId": "aclassoc-abcd1234",
    "NetworkAclId": "acl-021345abcdef6789",
    "SubnetId": "subnet-abcd1234"
  }],
  "Entries": [{
    "CidrBlock": "10.24.34.0/23",
    "Egress": true,
    "IcmpTypeCode": {
      "Code": 10,
      "Type": 30
    },
    "Ipv6CidrBlock": "2001:DB8::/32",
    "PortRange": {
      "From": 20,
      "To": 40
    }
  ]
}
```



```
    },
    "Protocol": "tcp",
    "RuleAction": "allow",
    "RuleNumber": 100
  }]
}
```

AwsEc2NetworkInterface

El `AwsEc2NetworkInterface` objeto proporciona información sobre una interfaz de EC2 red de Amazon.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2NetworkInterface` objeto. Para ver las descripciones de `AwsEc2NetworkInterface` los atributos, consulta el apartado [AwsEc2](#) de `NetworkInterfaceDetails` la referencia de la AWS Security Hub API.

Ejemplo

```
"AwsEc2NetworkInterface": {
  "Attachment": {
    "AttachTime": "2019-01-01T03:03:21Z",
    "AttachmentId": "eni-attach-43348162",
    "DeleteOnTermination": true,
    "DeviceIndex": 123,
    "InstanceId": "i-1234567890abcdef0",
    "InstanceOwnerId": "123456789012",
    "Status": 'ATTACHED'
  },
  "SecurityGroups": [
    {
      "GroupName": "my-security-group",
      "GroupId": "sg-903004f8"
    },
  ],
  "NetworkInterfaceId": 'eni-686ea200',
  "SourceDestCheck": false
}
```

AwsEc2RouteTable

El `AwsEc2RouteTable` objeto proporciona información sobre una tabla de EC2 rutas de Amazon.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2RouteTable` objeto. Para ver las descripciones de `AwsEc2RouteTable` los atributos, consulta el apartado [AwsEc2](#) de `RouteTableDetails` la referencia de la AWS Security Hub API.

Ejemplo

```
"AwsEc2RouteTable": {
  "AssociationSet": [{
    "AssociationSet": {
      "State": "associated"
    },
    "Main": true,
    "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
    "RouteTableId": "rtb-0a59bde9cf2548e34",
  }],
  "PropogatingVgwSet": [],
  "RouteTableId": "rtb-0a59bde9cf2548e34",
  "RouteSet": [
    {
      "DestinationCidrBlock": "10.24.34.0/23",
      "GatewayId": "local",
      "Origin": "CreateRouteTable",
      "State": "active"
    },
    {
      "DestinationCidrBlock": "10.24.34.0/24",
      "GatewayId": "igw-0242c2d7d513fc5d3",
      "Origin": "CreateRoute",
      "State": "active"
    }
  ],
  "VpcId": "vpc-0c250a5c33f51d456"
}
```

AwsEc2SecurityGroup

El `AwsEc2SecurityGroup` objeto describe un grupo de EC2 seguridad de Amazon.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2SecurityGroup` objeto. Para ver las descripciones de `AwsEc2SecurityGroup` los atributos, consulta el apartado [AwsEc2](#) de `SecurityGroupDetails` la referencia de la AWS Security Hub API.

Ejemplo

```
"AwsEc2SecurityGroup": {
  "GroupName": "MySecurityGroup",
  "GroupId": "sg-903004f8",
  "OwnerId": "123456789012",
  "VpcId": "vpc-1a2b3c4d",
  "IpPermissions": [
    {
      "IpProtocol": "-1",
      "IpRanges": [],
      "UserIdGroupPairs": [
        {
          "UserId": "123456789012",
          "GroupId": "sg-903004f8"
        }
      ],
      "PrefixListIds": [
        {"PrefixListId": "pl-63a5400a"}
      ]
    },
    {
      "PrefixListIds": [],
      "FromPort": 22,
      "IpRanges": [
        {
          "CidrIp": "203.0.113.0/24"
        }
      ],
      "ToPort": 22,
      "IpProtocol": "tcp",
      "UserIdGroupPairs": []
    }
  ]
}
```

AwsEc2Subnet

El `AwsEc2Subnet` objeto proporciona información sobre una subred de Amazon EC2.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2Subnet` objeto. Para ver las descripciones de `AwsEc2Subnet` los atributos, consulta el apartado [AwsEc2](#) de `SubnetDetails` la referencia de la AWS Security Hub API.

Ejemplo

```
AwsEc2Subnet: {
  "AssignIpv6AddressOnCreation": false,
  "AvailabilityZone": "us-west-2c",
  "AvailabilityZoneId": "usw2-az3",
  "AvailableIpAddressCount": 8185,
  "CidrBlock": "10.0.0.0/24",
  "DefaultForAz": false,
  "MapPublicIpOnLaunch": false,
  "OwnerId": "123456789012",
  "State": "available",
  "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/subnet-d5436c93",
  "SubnetId": "subnet-d5436c93",
  "VpcId": "vpc-153ade70",
  "Ipv6CidrBlockAssociationSet": [{
    "AssociationId": "subnet-cidr-assoc-EXAMPLE",
    "Ipv6CidrBlock": "2001:DB8::/32",
    "CidrBlockState": "associated"
  }]
}
```

AwsEc2TransitGateway

El `AwsEc2TransitGateway` objeto proporciona detalles sobre una pasarela de EC2 tránsito de Amazon que interconecta tus nubes privadas virtuales (VPCs) y tus redes locales.

El siguiente es un ejemplo de `AwsEc2TransitGateway` hallazgo en el formato de búsqueda AWS de seguridad (ASFF). Para ver las descripciones de `AwsEc2TransitGateway` los atributos, consulta la sección [AwsEc2](#) de `TransitGatewayDetails` la Referencia de la AWS Security Hub API.

Ejemplo

```
"AwsEc2TransitGateway": {
  "AmazonSideAsn": 65000,
  "AssociationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
  "AutoAcceptSharedAttachments": "disable",
  "DefaultRouteTableAssociation": "enable",
  "DefaultRouteTablePropagation": "enable",
  "Description": "sample transit gateway",
  "DnsSupport": "enable",
  "Id": "tgw-042ae6bf7a5c126c3",
```

```
"MulticastSupport": "disable",
"PropagationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
"TransitGatewayCidrBlocks": ["10.0.0.0/16"],
"VpnEcmpSupport": "enable"
}
```

AwsEc2Volume

El `AwsEc2Volume` objeto proporciona detalles sobre un EC2 volumen de Amazon.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2Volume` objeto. Para ver las descripciones de `AwsEc2Volume` los atributos, consulta el apartado [AwsEc2](#) de `VolumeDetails` la referencia de la AWS Security Hub API.

Ejemplo

```
"AwsEc2Volume": {
  "Attachments": [
    {
      "AttachTime": "2017-10-17T14:47:11Z",
      "DeleteOnTermination": true,
      "InstanceId": "i-123abc456def789g",
      "Status": "attached"
    }
  ],
  "CreateTime": "2020-02-24T15:54:30Z",
  "Encrypted": true,
  "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJa1rXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
  "Size": 80,
  "SnapshotId": "",
  "Status": "available"
}
```

AwsEc2Vpc

El `AwsEc2Vpc` objeto proporciona detalles sobre una Amazon EC2 VPC.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2Vpc` objeto. Para ver las descripciones de `AwsEc2Vpc` los atributos, consulta el apartado [AwsEc2](#) de `VpcDetails` la referencia de la AWS Security Hub API.

Ejemplo

```
"AwsEc2Vpc": {
  "CidrBlockAssociationSet": [
    {
      "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
      "CidrBlock": "192.0.2.0/24",
      "CidrBlockState": "associated"
    }
  ],
  "DhcpOptionsId": "dopt-4e42ce28",
  "Ipv6CidrBlockAssociationSet": [
    {
      "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
      "CidrBlockState": "associated",
      "Ipv6CidrBlock": "192.0.2.0/24"
    }
  ],
  "State": "available"
}
```

AwsEc2VpcEndpointService

El objeto `AwsEc2VpcEndpointService` contiene detalles sobre la configuración del servicio para un servicio de punto de conexión de VPC.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsEc2VpcEndpointService` objeto. Para ver las descripciones de `AwsEc2VpcEndpointService` los atributos, consulta el apartado [AwsEc2VpcEndpointServiceDetails](#) la referencia de la AWS Security Hub API.

Ejemplo

```
"AwsEc2VpcEndpointService": {
  "ServiceType": [
    {
      "ServiceType": "Interface"
    }
  ],
  "ServiceId": "vpce-svc-example1",
  "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example1",
}
```

```

    "ServiceState": "Available",
    "AvailabilityZones": [
        "us-east-1"
    ],
    "AcceptanceRequired": true,
    "ManagesVpcEndpoints": false,
    "NetworkLoadBalancerArns": [
        "arn:aws:elasticloadbalancing:us-east-1:444455556666:loadbalancer/net/my-network-load-balancer/example1"
    ],
    "GatewayLoadBalancerArns": [],
    "BaseEndpointDnsNames": [
        "vpce-svc-04eec859668b51c34.us-east-1.vpce.amazonaws.com"
    ],
    "PrivateDnsName": "my-private-dns"
}

```

AwsEc2VpcPeeringConnection

El `AwsEc2VpcPeeringConnection` objeto proporciona detalles sobre la conexión de red entre dos VPCs.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEc2VpcPeeringConnection` objeto. Para ver las descripciones de `AwsEc2VpcPeeringConnection` los atributos, consulta el apartado [AwsEc2](#) de `VpcPeeringConnectionDetails` la referencia de la AWS Security Hub API.

Ejemplo

```

"AwsEc2VpcPeeringConnection": {
  "AcceptorVpcInfo": {
    "CidrBlock": "10.0.0.0/28",
    "CidrBlockSet": [{
      "CidrBlock": "10.0.0.0/28"
    }],
    "Ipv6CidrBlockSet": [{
      "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
    }],
    "OwnerId": "012345678910",
    "PeeringOptions": {
      "AllowDnsResolutionFromRemoteVpc": true,
      "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
      "AllowEgressFromLocalVpcToRemoteClassicLink": true
    }
  }
}

```

```

    },
    "Region": "us-west-2",
    "VpcId": "vpc-i123456"
  },
  "ExpirationTime": "2022-02-18T15:31:53.161Z",
  "RequesterVpcInfo": {
    "CidrBlock": "192.168.0.0/28",
    "CidrBlockSet": [{
      "CidrBlock": "192.168.0.0/28"
    }],
    "Ipv6CidrBlockSet": [{
      "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
    }],
    "OwnerId": "012345678910",
    "PeeringOptions": {
      "AllowDnsResolutionFromRemoteVpc": true,
      "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
      "AllowEgressFromLocalVpcToRemoteClassicLink": true
    },
    "Region": "us-west-2",
    "VpcId": "vpc-i123456"
  },
  "Status": {
    "Code": "initiating-request",
    "Message": "Active"
  },
  "VpcPeeringConnectionId": "pcx-1a2b3c4d"
}

```

Recursos de AwsEcr en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los AwsEcr recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsEcrContainerImage

El objeto `AwsEcrContainerImage` proporciona información sobre una imagen de Amazon ECR.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsEcrContainerImage` objeto. Para ver las descripciones de los atributos

`AwsEcrContainerImage`, consulte [AwsEcrContainerImageDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEcrContainerImage": {
  "RegistryId": "123456789012",
  "RepositoryName": "repository-name",
  "Architecture": "amd64"
  "ImageDigest":
    "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
  "ImageTags": ["000000000-0000-0000-0000-000000000000"],
  "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

El objeto `AwsEcrRepository` proporciona información sobre un repositorio de Amazon Elastic Container Registry.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsEcrRepository` objeto. Para ver las descripciones de los atributos `AwsEcrRepository`, consulte [AwsEcrRepositoryDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEcrRepository": {
  "LifecyclePolicy": {
    "RegistryId": "123456789012",
  },
  "RepositoryName": "sample-repo",
  "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
  "ImageScanningConfiguration": {
    "ScanOnPush": true
  },
  "ImageTagMutability": "IMMUTABLE"
}
```

Recursos de AwsEcs en el ASFF

Los siguientes son ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsEcs` los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsEcsCluster

El objeto `AwsEcsCluster` proporciona detalles sobre un clúster de Amazon Elastic Container Service.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsEcsCluster` objeto. Para ver las descripciones de los atributos `AwsEcsCluster`, consulte [AwsEcsClusterDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEcsCluster": {
  "CapacityProviders": [],
  "ClusterSettings": [
    {
      "Name": "containerInsights",
      "Value": "enabled"
    }
  ],
  "Configuration": {
    "ExecuteCommandConfiguration": {
      "KmsKeyId": "kmsKeyId",
      "LogConfiguration": {
        "CloudWatchEncryptionEnabled": true,
        "CloudWatchLogGroupName": "cloudWatchLogGroupName",
        "S3BucketName": "s3BucketName",
        "S3EncryptionEnabled": true,
        "S3KeyPrefix": "s3KeyPrefix"
      },
      "Logging": "DEFAULT"
    },
    "DefaultCapacityProviderStrategy": [
      {
        "Base": 0,
        "CapacityProvider": "capacityProvider",
        "Weight": 1
      }
    ]
  }
}
```

AwsEcsContainer

El objeto de `AwsEcsContainer` contiene detalles sobre un contenedor Amazon ECS.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEcsContainer` objeto. Para ver las descripciones de los atributos `AwsEcsContainer`, consulte [AwsEcsContainerDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEcsContainer": {
  "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
    "ContainerPath": "/mnt/etc",
    "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
}
```

AwsEcsService

El objeto `AwsEcsService` proporciona detalles acerca de un servicio dentro de un clúster de Amazon ECS.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsEcsService` objeto. Para ver las descripciones de los atributos `AwsEcsService`, consulte [AwsEcsServiceDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEcsService": {
  "CapacityProviderStrategy": [
    {
      "Base": 12,
      "CapacityProvider": "",
      "Weight": ""
    }
  ],
  "Cluster": "arn:aws:ecs:us-east-1:111122223333:cluster/example-ecs-cluster",
  "DeploymentConfiguration": {
    "DeploymentCircuitBreaker": {
```

```
        "Enable": false,
        "Rollback": false
    },
    "MaximumPercent": 200,
    "MinimumHealthyPercent": 100
},
"DeploymentController": "",
"DesiredCount": 1,
"EnableEcsManagedTags": false,
"EnableExecuteCommand": false,
"HealthCheckGracePeriodSeconds": 1,
"LaunchType": "FARGATE",
"LoadBalancers": [
    {
        "ContainerName": "",
        "ContainerPort": 23,
        "LoadBalancerName": "",
        "TargetGroupArn": ""
    }
],
"Name": "sample-app-service",
"NetworkConfiguration": {
    "AwsVpcConfiguration": {
        "Subnets": [
            "Subnet-example1",
            "Subnet-example2"
        ],
        "SecurityGroups": [
            "Sg-0ce48e9a6e5b457f5"
        ],
        "AssignPublicIp": "ENABLED"
    }
},
"PlacementConstraints": [
    {
        "Expression": "",
        "Type": ""
    }
],
"PlacementStrategies": [
    {
        "Field": "",
        "Type": ""
    }
]
```

```

    ],
    "PlatformVersion": "LATEST",
    "PropagateTags": "",
    "Role": "arn:aws:iam::111122223333:role/aws-servicerole/ecs.amazonaws.com/ServiceRoleForECS",
    "SchedulingStrategy": "REPLICA",
    "ServiceName": "sample-app-service",
    "ServiceArn": "arn:aws:ecs:us-east-1:111122223333:service/example-ecs-cluster/sample-app-service",
    "ServiceRegistries": [
      {
        "ContainerName": "",
        "ContainerPort": 1212,
        "Port": 1221,
        "RegistryArn": ""
      }
    ],
    "TaskDefinition": "arn:aws:ecs:us-east-1:111122223333:task-definition/example-taskdef:1"
  }
}

```

AwsEcsTask

El objeto `AwsEcsTask` proporciona detalles sobre una tarea de Amazon ECS.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsEcsTask` objeto. Para ver las descripciones de los atributos `AwsEcsTask`, consulte [AwsEcsTask](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsEcsTask": {
  "ClusterArn": "arn:aws:ecs:us-west-2:123456789012:task/MyCluster/1234567890123456789",
  "CreatedAt": "1557134011644",
  "Group": "service:fargate-service",
  "StartedAt": "1557134011644",
  "StartedBy": "ecs-svc/1234567890123456789",
  "TaskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/sample-fargate:2",
  "Version": 3,
  "Volumes": [{
    "Name": "string",
    "Host": {

```

```

    "SourcePath": "string"
  }
}],
"Containers": {
  "Image": "11111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
    "ContainerPath": "/mnt/etc",
    "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
}
}

```

AwsEcsTaskDefinition

El objeto `AwsEcsTaskDefinition` contiene detalles sobre la definición de una tarea. Una definición de tarea describe las definiciones de contenedor y volumen de una tarea de Amazon Elastic Container Service.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsEcsTaskDefinition` objeto. Para ver las descripciones de los atributos `AwsEcsTaskDefinition`, consulte [AwsEcsTaskDefinitionDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsEcsTaskDefinition": {
  "ContainerDefinitions": [
    {
      "Command": ['ruby', 'hi.rb'],
      "Cpu": 128,
      "Essential": true,
      "HealthCheck": {
        "Command": ["CMD-SHELL", "curl -f http://localhost/ || exit 1"],
        "Interval": 10,
        "Retries": 3,
        "StartPeriod": 5,
        "Timeout": 20
      },
      "Image": "tongueroo/sinatra:latest",
    }
  ]
}

```

```

    "Interactive": true,
    "Links": [],
    "LogConfiguration": {
      "LogDriver": "awslogs",
      "Options": {
        "awslogs-group": "/ecs/sinatra-hi",
        "awslogs-region": "ap-southeast-1",
        "awslogs-stream-prefix": "ecs"
      },
      "SecretOptions": []
    },
    "MemoryReservation": 128,
    "Name": "web",
    "PortMappings": [
      {
        "ContainerPort": 4567,
        "HostPort": 4567,
        "Protocol": "tcp"
      }
    ],
    "Privileged": true,
    "StartTimeout": 10,
    "StopTimeout": 100,
  }
],
"Family": "sinatra-hi",
"NetworkMode": "host",
"RequiresCompatibilities": ["EC2"],
"Status": "ACTIVE",
"TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
}

```

Recursos de AwsEfs en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsEfs los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsEfsAccessPoint

El objeto `AwsEfsAccessPoint` proporciona detalles sobre los archivos almacenados en Amazon Elastic File System.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsEfsAccessPoint` objeto. Para ver las descripciones de los atributos `AwsEfsAccessPoint`, consulte [AwsEfsAccessPointDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEfsAccessPoint": {
  "AccessPointId": "fsap-05c4c0e79ba0b118a",
  "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/fsap-05c4c0e79ba0b118a",
  "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
  "FileSystemId": "fs-0f8137f731cb32146",
  "PosixUser": {
    "Gid": "1000",
    "SecondaryGids": ["0", "4294967295"],
    "Uid": "1234"
  },
  "RootDirectory": {
    "CreationInfo": {
      "OwnerGid": "1000",
      "OwnerUid": "1234",
      "Permissions": "777"
    },
    "Path": "/tmp/example"
  }
}
```

Recursos de AwsEks en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsEks` los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsEksCluster

El objeto `AwsEksCluster` proporciona detalles sobre un clúster de Amazon EKS.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsEksCluster` objeto. Para ver las descripciones de los atributos `AwsEksCluster`, consulte [AwsEksClusterDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
{
  "AwsEksCluster": {
    "Name": "example",
    "Arn": "arn:aws:eks:us-west-2:222222222222:cluster/example",
    "CreatedAt": 1565804921.901,
    "Version": "1.12",
    "RoleArn": "arn:aws:iam::222222222222:role/example-cluster-ServiceRole-1XWBQWYSFRE2Q",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": false,
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
    "Logging": {
      "ClusterLogging": [
        {
          "Types": [
            "api",
            "audit",
            "authenticator",
            "controllerManager",
            "scheduler"
          ],
          "Enabled": true
        }
      ]
    },
    "Status": "CREATING",
    "CertificateAuthorityData": {},
  }
}
```

Recursos de AwsElasticBeanstalk en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los recursos. `AwsElasticBeanstalk`

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

`AwsElasticBeanstalkEnvironment`

El objeto `AwsElasticBeanstalkEnvironment` contiene detalles sobre un entorno de AWS Elastic Beanstalk .

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsElasticBeanstalkEnvironment` objeto. Para ver las descripciones de los atributos `AwsElasticBeanstalkEnvironment`, consulte [AwsElasticBeanstalkEnvironmentDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsElasticBeanstalkEnvironment": {
  "ApplicationName": "MyApplication",
  "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
  "DateCreated": "2021-04-30T01:38:01.090Z",
  "DateUpdated": "2021-04-30T01:38:01.090Z",
  "Description": "Example description of my awesome application",
  "EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-east-1.elb.amazonaws.com",
  "EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/MyApplication/myapplication-env",
  "EnvironmentId": "e-abcd1234",
  "EnvironmentLinks": [
    {
      "EnvironmentName": "myexampleapp-env",
      "LinkName": "myapplicationLink"
    }
  ],
  "EnvironmentName": "myapplication-env",
  "OptionSettings": [
    {
      "Namespace": "aws:elasticbeanstalk:command",
      "OptionName": "BatchSize",
```

```

        "Value": "100"
      },
      {
        "Namespace": "aws:elasticbeanstalk:command",
        "OptionName": "Timeout",
        "Value": "600"
      },
      {
        "Namespace": "aws:elasticbeanstalk:command",
        "OptionName": "BatchSizeType",
        "Value": "Percentage"
      },
      {
        "Namespace": "aws:elasticbeanstalk:command",
        "OptionName": "IgnoreHealthCheck",
        "Value": "false"
      },
      {
        "Namespace": "aws:elasticbeanstalk:application",
        "OptionName": "Application Healthcheck URL",
        "Value": "TCP:80"
      }
    ],
    "PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
running on 64bit Amazon Linux/2.7.7",
    "SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
    "Status": "Ready",
    "Tier": {
      "Name": "WebServer"
      "Type": "Standard"
      "Version": "1.0"
    },
    "VersionLabel": "Sample Application"
  }
}

```

Recursos de AwsElasticSearch en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsElasticSearch los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsElasticSearchDomain

El `AwsElasticSearchDomain` objeto proporciona detalles sobre un dominio OpenSearch de Amazon Service.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsElasticSearchDomain` objeto. Para ver las descripciones de los atributos `AwsElasticSearchDomain`, consulte [AwsElasticSearchDomainDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsElasticSearchDomain": {
  "AccessPolicies": "string",
  "DomainStatus": {
    "DomainId": "string",
    "DomainName": "string",
    "Endpoint": "string",
    "Endpoints": {
      "string": "string"
    }
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": boolean,
    "TLSSecurityPolicy": "string"
  },
  "ElasticsearchClusterConfig": {
    "DedicatedMasterCount": number,
    "DedicatedMasterEnabled": boolean,
    "DedicatedMasterType": "string",
    "InstanceCount": number,
    "InstanceType": "string",
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": number
    },
    "ZoneAwarenessEnabled": boolean
  },
  "ElasticsearchVersion": "string",
  "EncryptionAtRestOptions": {
    "Enabled": boolean,
    "KmsKeyId": "string"
  },
  "LogPublishingOptions": {
```

```

    "AuditLogs": {
        "CloudWatchLogsLogGroupArn": "string",
        "Enabled": boolean
    },
    "IndexSlowLogs": {
        "CloudWatchLogsLogGroupArn": "string",
        "Enabled": boolean
    },
    "SearchSlowLogs": {
        "CloudWatchLogsLogGroupArn": "string",
        "Enabled": boolean
    }
},
"NodeToNodeEncryptionOptions": {
    "Enabled": boolean
},
"ServiceSoftwareOptions": {
    "AutomatedUpdateDate": "string",
    "Cancellable": boolean,
    "CurrentVersion": "string",
    "Description": "string",
    "NewVersion": "string",
    "UpdateAvailable": boolean,
    "UpdateStatus": "string"
},
"VPCOptions": {
    "AvailabilityZones": [
        "string"
    ],
    "SecurityGroupIds": [
        "string"
    ],
    "SubnetIds": [
        "string"
    ],
    "VPCId": "string"
}
}

```

Recursos de AwsElb en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsElb los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsElbLoadBalancer

El objeto `AwsElbLoadBalancer` contiene detalles sobre un Equilibrador de carga clásico.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsElbLoadBalancer` objeto. Para ver las descripciones de los atributos `AwsElbLoadBalancer`, consulte [AwsElbLoadBalancerDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsElbLoadBalancer": {
  "AvailabilityZones": ["us-west-2a"],
  "BackendServerDescriptions": [
    {
      "InstancePort": 80,
      "PolicyNames": ["doc-example-policy"]
    }
  ],
  "CanonicalHostedZoneName": "Z3DZXE0EXAMPLE",
  "CanonicalHostedZoneNameID": "my-load-balancer-444455556666.us-
west-2.elb.amazonaws.com",
  "CreatedTime": "2020-08-03T19:22:44.637Z",
  "DnsName": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
  "HealthCheck": {
    "HealthyThreshold": 2,
    "Interval": 30,
    "Target": "HTTP:80/png",
    "Timeout": 3,
    "UnhealthyThreshold": 2
  },
  "Instances": [
    {
      "InstanceId": "i-example"
    }
  ],
  "ListenerDescriptions": [
    {
      "Listener": {
        "InstancePort": 443,
        "InstanceProtocol": "HTTPS",
        "LoadBalancerPort": 443,
```

```

        "Protocol": "HTTPS",
        "SslCertificateId": "arn:aws:iam::444455556666:server-certificate/my-
server-cert"
    },
    "PolicyNames": ["ELBSecurityPolicy-TLS-1-2-2017-01"]
}
],
"LoadBalancerAttributes": {
    "AccessLog": {
        "EmitInterval": 60,
        "Enabled": true,
        "S3BucketName": "amzn-s3-demo-bucket",
        "S3BucketPrefix": "doc-example-prefix"
    },
    "ConnectionDraining": {
        "Enabled": false,
        "Timeout": 300
    },
    "ConnectionSettings": {
        "IdleTimeout": 30
    },
    "CrossZoneLoadBalancing": {
        "Enabled": true
    },
    "AdditionalAttributes": [{
        "Key": "elb.http.desyncmitigationmode",
        "Value": "strictest"
    }]
},
"LoadBalancerName": "example-load-balancer",
"Policies": {
    "AppCookieStickinessPolicies": [
        {
            "CookieName": "",
            "PolicyName": ""
        }
    ],
    "LbCookieStickinessPolicies": [
        {
            "CookieExpirationPeriod": 60,
            "PolicyName": "my-example-cookie-policy"
        }
    ]
},

```

```

    "OtherPolicies": [
        "my-PublicKey-policy",
        "my-authentication-policy",
        "my-SSLNegotiation-policy",
        "my-ProxyProtocol-policy",
        "ELBSecurityPolicy-2015-03"
    ],
    "Scheme": "internet-facing",
    "SecurityGroups": ["sg-example"],
    "SourceSecurityGroup": {
        "GroupName": "my-elb-example-group",
        "OwnerAlias": "444455556666"
    },
    "Subnets": ["subnet-example"],
    "VpcId": "vpc-a01106c2"
}

```

AwsElbv2LoadBalancer

El objeto `AwsElbv2LoadBalancer` proporciona información sobre un balanceador de carga.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsElbv2LoadBalancer` objeto. Para ver las descripciones de `AwsElbv2LoadBalancer` los atributos, consulta el apartado [AwsElbv2](#) de `LoadBalancerDetails` la referencia de la AWS Security Hub API.

Ejemplo

```

"AwsElbv2LoadBalancer": {
    "AvailabilityZones": {
        "SubnetId": "string",
        "ZoneName": "string"
    },
    "CanonicalHostedZoneId": "string",
    "CreatedTime": "string",
    "DNSName": "string",
    "IpAddressType": "string",
    "LoadBalancerAttributes": [
        {
            "Key": "string",
            "Value": "string"
        }
    ]
}

```



```
    ],  
    "Scheme": "string",  
    "SecurityGroups": [ "string" ],  
    "State": {  
        "Code": "string",  
        "Reason": "string"  
    },  
    "Type": "string",  
    "VpcId": "string"  
}
```

Recursos de AwsEventBridge en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsEventBridge los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsEventSchemasRegistry

El AwsEventSchemasRegistry objeto proporciona información sobre un registro de EventBridge esquemas de Amazon. Un esquema define la estructura de los eventos a los que se envían EventBridge. Los registros de esquemas son contenedores que recopilan y agrupan lógicamente sus esquemas.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del AwsEventSchemasRegistry objeto. Para ver las descripciones de los atributos AwsEventSchemasRegistry, consulte [AwsEventSchemasRegistry](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEventSchemasRegistry": {  
    "Description": "This is an example event schema registry.",  
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",  
    "RegistryName": "schema-registry"  
}
```

AwsEventsEndpoint

El `AwsEventsEndpoint` objeto proporciona información sobre un punto final EventBridge global de Amazon. Un punto de conexión puede mejorar la disponibilidad de su aplicación al hacerla tolerante a los fallos regionales.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEventsEndpoint` objeto. Para ver las descripciones de los atributos `AwsEventsEndpoint`, consulte [AwsEventsEndpointDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEventsEndpoint": {
  "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
  "Description": "This is a sample endpoint.",
  "EndpointId": "04k1exajoy.veo",
  "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
  "EventBuses": [
    {
      "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
    },
    {
      "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
    }
  ],
  "Name": "my-endpoint",
  "ReplicationConfig": {
    "State": "ENABLED"
  },
  "RoleArn": "arn:aws:iam::123456789012:role/service-role/Amazon_EventBridge_Invoke_Event_Bus_1258925394",
  "RoutingConfig": {
    "FailoverConfig": {
      "Primary": {
        "HealthCheck": "arn:aws:route53::healthcheck/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      },
      "Secondary": {
        "Route": "us-east-2"
      }
    }
  },
  "State": "ACTIVE"
}
```

}

AwsEventsEventbus

El `AwsEventsEventbus` objeto proporciona información sobre un punto final EventBridge global de Amazon. Un punto de conexión puede mejorar la disponibilidad de su aplicación al hacerla tolerante a los fallos regionales.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsEventsEventbus` objeto. Para ver las descripciones de los atributos `AwsEventsEventbus`, consulte [AwsEventsEventbusDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsEventsEventbus":
  "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
  "Name": "my-event-bus",
  "Policy": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n      \"Sid\":\n        \"AllowAllAccountsFromOrganizationToPutEvents\",\n      \"Effect\": \"Allow\",\n      \"Principal\": \"*\",\n      \"Action\": \"events:PutEvents\",\n      \"Resource\":\n        \"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\",\n      \"Condition\": {\n        \"StringEquals\": {\n          \"aws:PrincipalOrgID\": \"o-ki7yjdkjv5\"\n        }\n      },\n      \"Sid\":\n        \"AllowAccountToManageRulesTheyCreated\",\n      \"Effect\": \"Allow\",\n      \"Principal\": {\n        \"AWS\":\n          \"arn:aws:iam::123456789012:root\"\n      },\n      \"Action\": [\n        \"events:PutRule\",\n        \"events:PutTargets\",\n        \"events>DeleteRule\",\n        \"events:RemoveTargets\",\n        \"events:DisableRule\",\n        \"events:EnableRule\",\n        \"events:TagResource\",\n        \"events:UntagResource\",\n        \"events:DescribeRule\",\n        \"events>ListTargetsByRule\",\n        \"events>ListTagsForResource\"\n      ],\n      \"Resource\":\n        \"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\",\n      \"Condition\": {\n        \"StringEqualsIfExists\": {\n          \"events:creatorAccount\": \"123456789012\"\n        }\n      }\n    }\n  ]\n}"
```

Recursos de AwsGuardDuty en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsGuardDuty` los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsGuardDutyDetector

El `AwsGuardDutyDetector` objeto proporciona información sobre un GuardDuty detector de Amazon. Un detector es un objeto que representa el GuardDuty servicio. Se requiere un detector GuardDuty para que entre en funcionamiento.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsGuardDutyDetector` objeto. Para ver las descripciones de los atributos `AwsGuardDutyDetector`, consulte [AwsGuardDutyDetector](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsGuardDutyDetector": {
  "FindingPublishingFrequency": "SIX_HOURS",
  "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
  "Status": "ENABLED",
  "DataSources": {
    "CloudTrail": {
      "Status": "ENABLED"
    },
    "DnsLogs": {
      "Status": "ENABLED"
    },
    "FlowLogs": {
      "Status": "ENABLED"
    },
    "S3Logs": {
      "Status": "ENABLED"
    },
    "Kubernetes": {
      "AuditLogs": {
        "Status": "ENABLED"
      }
    },
    "MalwareProtection": {
      "ScanEc2InstanceWithFindings": {
        "EbsVolumes": {
          "Status": "ENABLED"
        }
      }
    }
  },
}
```

```

    "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-
    protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
  }
}

```

Recursos de AwsIam en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsIam` recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsIamAccessKey

El objeto `AwsIamAccessKey` contiene detalles sobre una clave de acceso de IAM relacionada con un resultado.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsIamAccessKey` objeto. Para ver las descripciones de los atributos `AwsIamAccessKey`, consulte [AwsIamAccessKeyDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsIamAccessKey": {
    "AccessKeyId": "string",
    "AccountId": "string",
    "CreatedAt": "string",
    "PrincipalId": "string",
    "PrincipalName": "string",
    "PrincipalType": "string",
    "SessionContext": {
        "Attributes": {
            "CreationDate": "string",
            "MfaAuthenticated": boolean
        },
        "SessionIssuer": {
            "AccountId": "string",
            "Arn": "string",
            "PrincipalId": "string",
            "Type": "string",
            "UserName": "string"
        }
    }
}

```

```
    }
  },
  "Status": "string"
}
```

AwsIamGroup

El objeto `AwsIamGroup` contiene detalles acerca de un grupo de IAM.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsIamGroup` objeto. Para ver las descripciones de los atributos `AwsIamGroup`, consulte [AwsIamGroupDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsIamGroup": {
  "AttachedManagedPolicies": [
    {
      "PolicyArn": "arn:aws:iam::aws:policy/ExampleManagedAccess",
      "PolicyName": "ExampleManagedAccess",
    }
  ],
  "CreateDate": "2020-04-28T14:08:37.000Z",
  "GroupId": "AGPA4TPS3VLP7QEXAMPLE",
  "GroupName": "Example_User_Group",
  "GroupPolicyList": [
    {
      "PolicyName": "ExampleGroupPolicy"
    }
  ],
  "Path": "/"
}
```

AwsIamPolicy

El objeto `AwsIamPolicy` representa una política de permisos de IAM.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsIamPolicy` objeto. Para ver las descripciones de los atributos `AwsIamPolicy`, consulte [AwsIamPolicyDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsIamPolicy": {
  "AttachmentCount": 1,
  "CreateDate": "2017-09-14T08:17:29.000Z",
  "DefaultVersionId": "v1",
  "Description": "Example IAM policy",
  "IsAttachable": true,
  "Path": "/",
  "PermissionsBoundaryUsageCount": 5,
  "PolicyId": "ANPAJ2UCCR6DPCEXAMPLE",
  "PolicyName": "EXAMPLE-MANAGED-POLICY",
  "PolicyVersionList": [
    {
      "VersionId": "v1",
      "IsDefaultVersion": true,
      "CreateDate": "2017-09-14T08:17:29.000Z"
    }
  ],
  "UpdateDate": "2017-09-14T08:17:29.000Z"
}
```

AwsIamRole

El objeto `AwsIamRole` contiene información sobre un rol de IAM, incluidas todas las políticas del rol.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsIamRole` objeto. Para ver las descripciones de los atributos `AwsIamRole`, consulte [AwsIamRoleDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsIamRole": {
  "AssumeRolePolicyDocument": "{ 'Version': '2012-10-17', 'Statement': [{ 'Effect': 'Allow', 'Action': 'sts:AssumeRole' } ] }",
  "AttachedManagedPolicies": [
    {
      "PolicyArn": "arn:aws:iam::aws:policy/ExamplePolicy1",
      "PolicyName": "Example policy 1"
    },
    {
      "PolicyArn": "arn:aws:iam::444455556666:policy/ExamplePolicy2",
      "PolicyName": "Example policy 2"
    }
  ],
}
```

```

    "CreateDate": "2020-03-14T07:19:14.000Z",
    "InstanceProfileList": [
      {
        "Arn": "arn:aws:iam::333333333333:ExampleProfile",
        "CreateDate": "2020-03-11T00:02:27Z",
        "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
        "InstanceProfileName": "ExampleInstanceProfile",
        "Path": "/",
        "Roles": [
          {
            "Arn": "arn:aws:iam::444455556666:role/example-role",
            "AssumeRolePolicyDocument": "",
            "CreateDate": "2020-03-11T00:02:27Z",
            "Path": "/",
            "RoleId": "AR0AJ520TH4H7LEXAMPLE",
            "RoleName": "example-role",
          }
        ]
      }
    ],
    "MaxSessionDuration": 3600,
    "Path": "/",
    "PermissionsBoundary": {
      "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
      "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
    },
    "RoleId": "AR0A4TPS3VLEXAMPLE",
    "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
    "RolePolicyList": [
      {
        "PolicyName": "Example role policy"
      }
    ]
  }
}

```

AwsIamUser

El objeto `AwsIamUser` proporciona información sobre un usuario.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsIamUser` objeto. Para ver las descripciones de los atributos `AwsIamUser`, consulte [AwsIamUserDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo


```

"AwsIamUser": {
  "AttachedManagedPolicies": [
    {
      "PolicyName": "ExamplePolicy",
      "PolicyArn": "arn:aws:iam::aws:policy/ExampleAccess"
    }
  ],
  "CreateDate": "2018-01-26T23:50:05.000Z",
  "GroupList": [],
  "Path": "/",
  "PermissionsBoundary" : {
    "PermissionsBoundaryArn" : "arn:aws:iam::aws:policy/AdministratorAccess",
    "PermissionsBoundaryType" : "PermissionsBoundaryPolicy"
  },
  "UserId": "AIDACKCEVSQ6C2EXAMPLE",
  "UserName": "ExampleUser",
  "UserPolicyList": [
    {
      "PolicyName": "InstancePolicy"
    }
  ]
}

```

Recursos de AwsKinesis en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los AwsKinesis recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsKinesisStream

El objeto `AwsKinesisStream` proporciona detalles sobre Amazon Kinesis Data Streams.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsKinesisStream` objeto. Para ver las descripciones de los atributos `AwsKinesisStream`, consulte [AwsKinesisStreamDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsKinesisStream": {
  "Name": "test-vir-kinesis-stream",

```

```

"Arn": "arn:aws:kinesis:us-east-1:293279581038:stream/test-vir-kinesis-stream",
"RetentionPeriodHours": 24,
"ShardCount": 2,
"StreamEncryption": {
  "EncryptionType": "KMS",
  "KeyId": "arn:aws:kms:us-east-1:293279581038:key/849cf029-4143-4c59-91f8-
ea76007247eb"
}
}

```

Recursos de AwsKms en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsKms los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsKmsKey

El AwsKmsKey objeto proporciona detalles sobre un AWS KMS key.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del AwsKmsKey objeto. Para ver las descripciones de los atributos AwsKmsKey, consulte [AwsKmsKeyDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsKmsKey": {
    "AWSAccountId": "string",
    "CreationDate": "string",
    "Description": "string",
    "KeyId": "string",
    "KeyManager": "string",
    "KeyRotationStatus": boolean,
    "KeyState": "string",
    "Origin": "string"
}

```

AwsLambda

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los AwsLambda recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsLambdaFunction

El objeto `AwsLambdaFunction` proporciona detalles sobre la configuración de una función de Lambda.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsLambdaFunction` objeto. Para ver las descripciones de los atributos `AwsLambdaFunction`, consulte [AwsLambdaFunctionDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsLambdaFunction": {
    "Architectures": [
        "x86_64"
    ],
    "Code": {
        "S3Bucket": "amzn-s3-demo-bucket",
        "S3Key": "samplekey",
        "S3ObjectVersion": "2",
        "ZipFile": "myzip.zip"
    },
    "CodeSha256": "1111111111111111abcdef",
    "DeadLetterConfig": {
        "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
    },
    "Environment": {
        "Variables": {
            "Stage": "foobar"
        },
        "Error": {
            "ErrorCode": "Sample-error-code",
            "Message": "Caller principal is a manager."
        }
    },
    "FunctionName": "CheckOut",
    "Handler": "main.py:lambda_handler",
    "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
    "LastModified": "2001-09-11T09:00:00Z",
    "Layers": {
        "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
```

```
    "CodeSize": 169
  },
  "PackageType": "Zip",
  "RevisionId": "23",
  "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
  "Runtime": "go1.7",
  "Timeout": 15,
  "TracingConfig": {
    "Mode": "Active"
  },
  "Version": "$LATEST",
  "VpcConfig": {
    "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
    "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
  },
  "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
  "MemorySize": 2048
}
```

AwsLambdaLayerVersion

El objeto `AwsLambdaLayerVersion` proporciona detalles sobre una versión de la capa de Lambda.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsLambdaLayerVersion` objeto. Para ver las descripciones de los atributos `AwsLambdaLayerVersion`, consulte [AwsLambdaLayerVersionDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsLambdaLayerVersion": {
  "Version": 2,
  "CompatibleRuntimes": [
    "java8"
  ],
  "CreateDate": "2019-10-09T22:02:00.274+0000"
}
```

Recursos de AwsMsk en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsMsk` recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsMskCluster

El objeto `AwsMskCluster` proporciona información sobre un clúster de Amazon Managed Streaming para Apache Kafka (Amazon MSK).

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsMskCluster` objeto. Para ver las descripciones de los atributos `AwsMskCluster`, consulte [AwsMskClusterDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsMskCluster": {
  "ClusterInfo": {
    "ClientAuthentication": {
      "Sasl": {
        "Scram": {
          "Enabled": true
        },
        "Iam": {
          "Enabled": true
        }
      },
      "Tls": {
        "CertificateAuthorityArnList": [],
        "Enabled": false
      },
      "Unauthenticated": {
        "Enabled": false
      }
    },
    "ClusterName": "my-cluster",
    "CurrentVersion": "K2PWKAKR8XB7XF",
    "EncryptionInfo": {
      "EncryptionAtRest": {
        "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      },
      "EncryptionInTransit": {
        "ClientBroker": "TLS",
        "InCluster": true
      }
    }
  }
}
```

```

        }
    },
    "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
    "NumberOfBrokerNodes": 3
}
}

```

Recursos de AwsNetworkFirewall en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsNetworkFirewall` los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsNetworkFirewallFirewall

El objeto `AwsNetworkFirewallFirewall` contiene detalles acerca de un firewall AWS Network Firewall .

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsNetworkFirewallFirewall` objeto. Para ver las descripciones de los atributos `AwsNetworkFirewallFirewall`, consulte [AwsNetworkFirewallFirewallDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsNetworkFirewallFirewall": {
    "DeleteProtection": false,
    "FirewallArn": "arn:aws:network-firewall:us-east-1:024665936331:firewall/testfirewall",
    "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-policy/InitialFirewall",
    "FirewallId": "dea7d8e9-ae38-4a8a-b022-672a830a99fa",
    "FirewallName": "testfirewall",
    "FirewallPolicyChangeProtection": false,
    "SubnetChangeProtection": false,
    "SubnetMappings": [
        {
            "SubnetId": "subnet-0183481095e588cdc"
        },
        {

```

```

        "SubnetId": "subnet-01f518fad1b1c90b0"
    }
],
    "VpcId": "vpc-40e83c38"
}

```

AwsNetworkFirewallFirewallPolicy

El objeto `AwsNetworkFirewallFirewallPolicy` proporciona detalles sobre una política de firewall. Una política de firewall define el comportamiento de un firewall de red.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsNetworkFirewallFirewallPolicy` objeto. Para ver las descripciones de los atributos `AwsNetworkFirewallFirewallPolicy`, consulte [AwsNetworkFirewallFirewallPolicyDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsNetworkFirewallFirewallPolicy": {
    "FirewallPolicy": {
        "StatefulRuleGroupReferences": [
            {
                "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-rulegroup/PatchesOnly"
            }
        ],
        "StatelessDefaultActions": [ "aws:forward_to_sfe" ],
        "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ],
        "StatelessRuleGroupReferences": [
            {
                "Priority": 1,
                "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-rulegroup/Stateless-1"
            }
        ]
    },
    "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-policy/InitialFirewall",
    "FirewallPolicyId": "9ceeda22-6050-4048-a0ca-50ce47f0cc65",
    "FirewallPolicyName": "InitialFirewall",
    "Description": "Initial firewall"
}

```

AwsNetworkFirewallRuleGroup

El objeto `AwsNetworkFirewallRuleGroup` proporciona detalles sobre un grupo de reglas AWS Network Firewall . Los grupos de reglas se utilizan para inspeccionar y controlar el tráfico de red. Los grupos de reglas sin estado se aplican a paquetes individuales. Los grupos de reglas con estado se aplican a los paquetes en el contexto de su flujo de tráfico.

En las políticas de firewall se hace referencia a los grupos de reglas.

Los ejemplos siguientes muestran el formato AWS de búsqueda de seguridad (ASFF) del `AwsNetworkFirewallRuleGroup` objeto. Para ver las descripciones de los atributos `AwsNetworkFirewallRuleGroup`, consulte [AwsNetworkFirewallRuleGroupDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo: grupo de reglas sin estado

```
"AwsNetworkFirewallRuleGroup": {
  "Capacity": 600,
  "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-rulegroup/Stateless-1",
  "RuleGroupId": "fb13c4df-b6da-4c1e-91ec-84b7a5487493",
  "RuleGroupName": "Stateless-1"
  "Description": "Example of a stateless rule group",
  "Type": "STATELESS",
  "RuleGroup": {
    "RulesSource": {
      "StatelessRulesAndCustomActions": {
        "CustomActions": [],
        "StatelessRules": [
          {
            "Priority": 1,
            "RuleDefinition": {
              "Actions": [
                "aws:pass"
              ],
              "MatchAttributes": {
                "DestinationPorts": [
                  {
                    "FromPort": 443,
                    "ToPort": 443
                  }
                ]
              }
            }
          }
        ],
        "Destinations": [
```



```
{
    {
        "AddressDefinition": "192.0.2.0/24"
    },
    "Protocols": [
        6
    ],
    "SourcePorts": [
        {
            "FromPort": 0,
            "ToPort": 65535
        }
    ],
    "Sources": [
        {
            "AddressDefinition": "198.51.100.0/24"
        }
    ]
}
}
```

Ejemplo: grupo de reglas con estado

```
"AwsNetworkFirewallRuleGroup": {
  "Capacity": 100,
  "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-rulegroup/tupletest",
  "RuleGroupId": "38b71c12-da80-4643-a6c5-03337f8933e0",
  "RuleGroupName": "ExampleRuleGroup",
  "Description": "Example of a stateful rule group",
  "Type": "STATEFUL",
  "RuleGroup": {
    "RuleSource": {
      "StatefulRules": [
        {
          "Action": "PASS",
          "Header": {
```

```
        "Destination": "Any",
        "DestinationPort": "443",
        "Direction": "ANY",
        "Protocol": "TCP",
        "Source": "Any",
        "SourcePort": "Any"
    },
    "RuleOptions": [
        {
            "Keyword": "sid:1"
        }
    ]
}
}
```

La siguiente es una lista de ejemplos de valores válidos para los atributos `AwsNetworkFirewallRuleGroup`:

- Action

Valores válidos: PASS | DROP | ALERT

- Protocol

Valores válidos: IP | TCP | UDP | ICMP | HTTP | FTP | TLS | SMB | DNS | DCERPC | SSH | SMTP | IMAP | MSN | KRB5 | IKEV2 | TFTP | NTP | DHCP

- Flags

Valores válidos: FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

- Masks

Valores válidos: FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

Recursos de AwsOpenSearchService en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsOpenSearchService` los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsOpenSearchServiceDomain

El `AwsOpenSearchServiceDomain` objeto contiene información sobre un dominio OpenSearch de Amazon Service.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsOpenSearchServiceDomain` objeto. Para ver las descripciones de los atributos `AwsOpenSearchServiceDomain`, consulte [AwsOpenSearchServiceDomainDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsOpenSearchServiceDomain": {
  "AccessPolicies": "IAM_Id",
  "AdvancedSecurityOptions": {
    "Enabled": true,
    "InternalUserDatabaseEnabled": true,
    "MasterUserOptions": {
      "MasterUserArn": "arn:aws:iam::123456789012:user/third-master-use",
      "MasterUserName": "third-master-use",
      "MasterUserPassword": "some-password"
    }
  },
  "Arn": "arn:aws:opensearch:us-east-1:111122223333:somedomain",
  "ClusterConfig": {
    "InstanceType": "c5.large.search",
    "InstanceCount": 1,
    "DedicatedMasterEnabled": true,
    "ZoneAwarenessEnabled": false,
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 2
    },
    "DedicatedMasterType": "c5.large.search",
    "DedicatedMasterCount": 3,
    "WarmEnabled": true,
    "WarmCount": 3,
    "WarmType": "ultrawarm1.large.search"
  },
  "DomainEndpoint": "https://es-2021-06-23t17-04-qowmgghud5vofgb5e4wmi.eu-central-1.es.amazonaws.com",
```

```

"DomainEndpointOptions": {
  "EnforceHTTPS": false,
  "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07",
  "CustomEndpointCertificateArn": "arn:aws:acm:us-east-1:111122223333:certificate/bda1bff1-79c0-49d0-abe6-50a15a7477d4",
  "CustomEndpointEnabled": true,
  "CustomEndpoint": "example.com"
},
"DomainEndpoints": {
  "vpc": "vpc-endpoint-h2dsd34efgyghrtguk5gt6j2foh4.us-east-1.es.amazonaws.com"
},
"DomainName": "my-domain",
"EncryptionAtRestOptions": {
  "Enabled": false,
  "KmsKeyId": "1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a"
},
"EngineVersion": "7.1",
"Id": "123456789012",
"LogPublishingOptions": {
  "IndexSlowLogs": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-group:/aws/aes/domains/es-index-slow-logs",
    "Enabled": true
  },
  "SearchSlowLogs": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-group:/aws/aes/domains/es-slow-logs",
    "Enabled": true
  },
  "AuditLogs": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-group:/aws/aes/domains/es-slow-logs",
    "Enabled": true
  }
},
"NodeToNodeEncryptionOptions": {
  "Enabled": true
},
"ServiceSoftwareOptions": {
  "AutomatedUpdateDate": "2022-04-28T14:08:37.000Z",
  "Cancellable": false,
  "CurrentVersion": "R20210331",
  "Description": "There is no software update available for this domain.",
  "NewVersion": "OpenSearch_1.0",

```

```

        "UpdateAvailable": false,
        "UpdateStatus": "COMPLETED",
        "OptionalDeployment": false
    },
    "VpcOptions": {
        "SecurityGroupIds": [
            "sg-2a3a4a5a"
        ],
        "SubnetIds": [
            "subnet-1a2a3a4a"
        ],
    }
}

```

Recursos de AwsRds en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los AwsRds recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsRdsDbCluster

El objeto `AwsRdsDbCluster` proporciona detalles sobre un clúster de base de datos de Amazon RDS.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsRdsDbCluster` objeto. Para ver las descripciones de los atributos `AwsRdsDbCluster`, consulte [AwsRdsDbClusterDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsRdsDbCluster": {
    "ActivityStreamStatus": "stopped",
    "AllocatedStorage": 1,
    "AssociatedRoles": [
        {
            "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/AWSServiceRoleForRDS",
            "Status": "PENDING"
        }
    ],
}

```

```
"AutoMinorVersionUpgrade": true,
"AvailabilityZones": [
  "us-east-1a",
  "us-east-1c",
  "us-east-1e"
],
"BackupRetentionPeriod": 1,
"ClusterCreateTime": "2020-06-22T17:40:12.322Z",
"CopyTagsToSnapshot": true,
"CrossAccountClone": false,
"CustomEndpoints": [],
"DatabaseName": "Sample name",
"DbClusterIdentifier": "database-3",
"DbClusterMembers": [
  {
    "DbClusterParameterGroupStatus": "in-sync",
    "DbInstanceIdentifier": "database-3-instance-1",
    "IsClusterWriter": true,
    "PromotionTier": 1,
  }
],
"DbClusterOptionGroupMemberships": [],
"DbClusterParameterGroup": "cluster-parameter-group",
"DbClusterResourceId": "cluster-example",
"DbSubnetGroup": "subnet-group",
"DeletionProtection": false,
"DomainMemberships": [],
"Status": "modifying",
"EnabledCloudwatchLogsExports": [
  "audit",
  "error",
  "general",
  "slowquery"
],
"Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
"Engine": "aurora-mysql",
"EngineMode": "provisioned",
"EngineVersion": "5.7.mysql_aurora.2.03.4",
"HostedZoneId": "ZONE1",
"HttpEndpointEnabled": false,
"IamDatabaseAuthenticationEnabled": false,
"KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
"MasterUsername": "admin",
"MultiAz": false,
```

```

    "Port": 3306,
    "PreferredBackupWindow": "04:52-05:22",
    "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
    "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
    "ReadReplicaIdentifiers": [],
    "Status": "Modifying",
    "StorageEncrypted": true,
    "VpcSecurityGroups": [
      {
        "Status": "active",
        "VpcSecurityGroupId": "sg-example-1"
      }
    ],
  }
}

```

AwsRdsDbClusterSnapshot

El objeto `AwsRdsDbClusterSnapshot` contiene información acerca de una instantánea de clúster de base de datos de Amazon RDS.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsRdsDbClusterSnapshot` objeto. Para ver las descripciones de los atributos `AwsRdsDbClusterSnapshot`, consulte [AwsRdsDbClusterSnapshotDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsRdsDbClusterSnapshot": {
  "AllocatedStorage": 0,
  "AvailabilityZones": [
    "us-east-1a",
    "us-east-1d",
    "us-east-1e"
  ],
  "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
  "DbClusterIdentifier": "database-2",
  "DbClusterSnapshotAttributes": [{
    "AttributeName": "restore",
    "AttributeValues": ["123456789012"]
  }],
  "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
  "Engine": "aurora",
  "EngineVersion": "5.6.10a",

```

```

    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "LicenseModel": "aurora",
    "MasterUsername": "admin",
    "PercentProgress": 100,
    "Port": 0,
    "SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
    "SnapshotType": "automated",
    "Status": "available",
    "StorageEncrypted": true,
    "VpcId": "vpc-faf7e380"
  }

```

AwsRdsDbInstance

El objeto `AwsRdsDbInstance` proporciona detalles sobre una instancia de base de datos de RDS de Amazon.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsRdsDbInstance` objeto. Para ver las descripciones de los atributos `AwsRdsDbInstance`, consulte [AwsRdsDbInstanceDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsRdsDbInstance": {
  "AllocatedStorage": 20,
  "AssociatedRoles": [],
  "AutoMinorVersionUpgrade": true,
  "AvailabilityZone": "us-east-1d",
  "BackupRetentionPeriod": 7,
  "CaCertificateIdentifier": "certificate1",
  "CharacterSetName": "",
  "CopyTagsToSnapshot": true,
  "DbClusterIdentifier": "",
  "DbInstanceArn": "arn:aws:rds:us-east-1:111122223333:db:database-1",
  "DbInstanceClass": "db.t2.micro",
  "DbInstanceIdentifier": "database-1",
  "DbInstancePort": 0,
  "DbInstanceStatus": "available",
  "DbiResourceId": "db-EXAMPLE123",
  "DbName": "",
  "DbParameterGroups": [
    {

```



```

        "DbParameterGroupName": "default.mysql5.7",
        "ParameterApplyStatus": "in-sync"
    }
],
"DbSecurityGroups": [],

"DbSubnetGroup": {
    "DbSubnetGroupName": "my-group-123abc",
    "DbSubnetGroupDescription": "My subnet group",
    "VpcId": "vpc-example1",
    "SubnetGroupStatus": "Complete",
    "Subnets": [
        {
            "SubnetIdentifier": "subnet-123abc",
            "SubnetAvailabilityZone": {
                "Name": "us-east-1d"
            },
            "SubnetStatus": "Active"
        },
        {
            "SubnetIdentifier": "subnet-456def",
            "SubnetAvailabilityZone": {
                "Name": "us-east-1c"
            },
            "SubnetStatus": "Active"
        }
    ],
    "DbSubnetGroupArn": ""
},
"DeletionProtection": false,
"DomainMemberships": [],
"EnabledCloudWatchLogsExports": [],
"Endpoint": {
    "address": "database-1.example.us-east-1.rds.amazonaws.com",
    "port": 3306,
    "hostedZoneId": "ZONEID1"
},
"Engine": "mysql",
"EngineVersion": "5.7.22",
"EnhancedMonitoringResourceArn": "arn:aws:logs:us-east-1:111122223333:log-
group:Example:log-stream:db-EXAMPLE1",
"IamDatabaseAuthenticationEnabled": false,
"InstanceCreateTime": "2020-06-22T17:40:12.322Z",

```

```

"Iops": "",
"KmsKeyId": "",
"LatestRestorableTime": "2020-06-24T05:50:00.000Z",
"LicenseModel": "general-public-license",
"ListenerEndpoint": "",
"MasterUsername": "admin",
"MaxAllocatedStorage": 1000,
"MonitoringInterval": 60,
"MonitoringRoleArn": "arn:aws:iam::111122223333:role/rds-monitoring-role",
"MultiAz": false,
"OptionGroupMemberships": [
  {
    "OptionGroupName": "default:mysql-5-7",
    "Status": "in-sync"
  }
],
"PreferredBackupWindow": "03:57-04:27",
"PreferredMaintenanceWindow": "thu:10:13-thu:10:43",
"PendingModifiedValues": {
  "DbInstanceClass": "",
  "AllocatedStorage": "",
  "MasterUserPassword": "",
  "Port": "",
  "BackupRetentionPeriod": "",
  "MultiAZ": "",
  "EngineVersion": "",
  "LicenseModel": "",
  "Iops": "",
  "DbInstanceIdentifier": "",
  "StorageType": "",
  "CaCertificateIdentifier": "",
  "DbSubnetGroupName": "",
  "PendingCloudWatchLogsExports": "",
  "ProcessorFeatures": []
},
"PerformanceInsightsEnabled": false,
"PerformanceInsightsKmsKeyId": "",
"PerformanceInsightsRetentionPeriod": "",
"ProcessorFeatures": [],
"PromotionTier": "",
"PubliclyAccessible": false,
"ReadReplicaDBClusterIdentifiers": [],
"ReadReplicaDBInstanceIdentifiers": [],
"ReadReplicaSourceDBInstanceIdentifier": "",

```

```

    "SecondaryAvailabilityZone": "",
    "StatusInfos": [],
    "StorageEncrypted": false,
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Timezone": "",
    "VpcSecurityGroups": [
      {
        "VpcSecurityGroupId": "sg-example1",
        "Status": "active"
      }
    ]
  }
}

```

AwsRdsDbSecurityGroup

El objeto `AwsRdsDbSecurityGroup` contiene información sobre Amazon Relational Database Service (RDS).

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsRdsDbSecurityGroup` objeto. Para ver las descripciones de los atributos `AwsRdsDbSecurityGroup`, consulte [AwsRdsDbSecurityGroupDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsRdsDbSecurityGroup": {
  "DbSecurityGroupArn": "arn:aws:rds:us-west-1:111122223333:secgrp:default",
  "DbSecurityGroupDescription": "default",
  "DbSecurityGroupName": "mysecgroup",
  "Ec2SecurityGroups": [
    {
      "Ec2SecurityGrouppuId": "myec2group",
      "Ec2SecurityGroupName": "default",
      "Ec2SecurityGroupOwnerId": "987654321021",
      "Status": "authorizing"
    }
  ],
  "IpRanges": [
    {
      "Cidrip": "0.0.0.0/0",
      "Status": "authorizing"
    }
  ]
}

```

```
  ],  
  "OwnerId": "123456789012",  
  "VpcId": "vpc-1234567f"  
}
```

AwsRdsDbSnapshot

El objeto `AwsRdsDbSnapshot` contiene detalles acerca de una instantánea de clúster de base de datos de Amazon RDS.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsRdsDbSnapshot` objeto. Para ver las descripciones de los atributos `AwsRdsDbSnapshot`, consulte [AwsRdsDbSnapshotDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsRdsDbSnapshot": {  
  "DbSnapshotIdentifier": "rds:database-1-2020-06-22-17-41",  
  "DbInstanceIdentifier": "database-1",  
  "SnapshotCreateTime": "2020-06-22T17:41:29.967Z",  
  "Engine": "mysql",  
  "AllocatedStorage": 20,  
  "Status": "available",  
  "Port": 3306,  
  "AvailabilityZone": "us-east-1d",  
  "VpcId": "vpc-example1",  
  "InstanceCreateTime": "2020-06-22T17:40:12.322Z",  
  "MasterUsername": "admin",  
  "EngineVersion": "5.7.22",  
  "LicenseModel": "general-public-license",  
  "SnapshotType": "automated",  
  "Iops": null,  
  "OptionGroupName": "default:mysql-5-7",  
  "PercentProgress": 100,  
  "SourceRegion": null,  
  "SourceDbSnapshotIdentifier": "",  
  "StorageType": "gp2",  
  "TdeCredentialArn": "",  
  "Encrypted": false,  
  "KmsKeyId": "",  
  "Timezone": "",  
  "IamDatabaseAuthenticationEnabled": false,  
  "ProcessorFeatures": [],  
}
```

```
"DbiResourceId": "db-resourceexample1"
}
```

AwsRdsEventSubscription

`AwsRdsEventSubscription` contiene detalles sobre una suscripción de notificación de eventos de RDS. La suscripción permite a RDS publicar eventos en un tema de SNS.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsRdsEventSubscription` objeto. Para ver las descripciones de los atributos `AwsRdsEventSubscription`, consulte [AwsRdsEventSubscriptionDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsRdsEventSubscription": {
  "CustSubscriptionId": "myawsuser-secgrp",
  "CustomerAwsId": "111111111111",
  "Enabled": true,
  "EventCategoriesList": [
    "configuration change",
    "failure"
  ],
  "EventSubscriptionArn": "arn:aws:rds:us-east-1:111111111111:es:my-instance-events",
  "SnsTopicArn": "arn:aws:sns:us-east-1:111111111111:myawsuser-RDS",
  "SourceIdsList": [
    "si-sample",
    "mysqldb-rr"
  ],
  "SourceType": "db-security-group",
  "Status": "creating",
  "SubscriptionCreationTime": "2021-06-27T01:38:01.090Z"
}
```

Recursos de AwsRedshift en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los `AwsRedshift` recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsRedshiftCluster

El objeto `AwsRedshiftCluster` contiene detalles sobre un clúster de Amazon Redshift.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsRedshiftCluster` objeto. Para ver las descripciones de los atributos `AwsRedshiftCluster`, consulte [AwsRedshiftClusterDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsRedshiftCluster": {
  "AllowVersionUpgrade": true,
  "AutomatedSnapshotRetentionPeriod": 1,
  "AvailabilityZone": "us-west-2d",
  "ClusterAvailabilityStatus": "Unavailable",
  "ClusterCreateTime": "2020-08-03T19:22:44.637Z",
  "ClusterIdentifier": "redshift-cluster-1",
  "ClusterNodes": [
    {
      "NodeRole": "LEADER",
      "PrivateIPAddress": "192.0.2.108",
      "PublicIPAddress": "198.51.100.29"
    },
    {
      "NodeRole": "COMPUTE-0",
      "PrivateIPAddress": "192.0.2.22",
      "PublicIPAddress": "198.51.100.63"
    },
    {
      "NodeRole": "COMPUTE-1",
      "PrivateIPAddress": "192.0.2.224",
      "PublicIPAddress": "198.51.100.226"
    }
  ],
  "ClusterParameterGroups": [
    {
      "ClusterParameterStatusList": [
        {
          "ParameterName": "max_concurrency_scaling_clusters",
          "ParameterApplyStatus": "in-sync",
          "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
        },
        {
          "ParameterName": "enable_user_activity_logging",
```

```

        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
        "ParameterName": "auto_analyze",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
        "ParameterName": "query_group",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
        "ParameterName": "datestyle",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
        "ParameterName": "extra_float_digits",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
        "ParameterName": "search_path",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
        "ParameterName": "statement_timeout",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
        "ParameterName": "wlm_json_configuration",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
        "ParameterName": "require_ssl",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {

```

```

        "ParameterName": "use_fips_ssl",
        "ParameterApplyStatus": "in-sync",
        "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    }
],
    "ParameterApplyStatus": "in-sync",
    "ParameterGroupName": "temp"
}
],
"ClusterPublicKey": "JalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
"ClusterRevisionNumber": 17498,
"ClusterSecurityGroups": [
    {
        "ClusterSecurityGroupName": "default",
        "Status": "active"
    }
],
"ClusterSnapshotCopyStatus": {
    "DestinationRegion": "us-west-2",
    "ManualSnapshotRetentionPeriod": -1,
    "RetentionPeriod": 1,
    "SnapshotCopyGrantName": "snapshotCopyGrantName"
},
"ClusterStatus": "available",
"ClusterSubnetGroupName": "default",
"ClusterVersion": "1.0",
"DBName": "dev",
"DeferredMaintenanceWindows": [
    {
        "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
        "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
        "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
    }
],
"ElasticIpStatus": {
    "ElasticIp": "203.0.113.29",
    "Status": "active"
},
"ElasticResizeNumberOfNodeOptions": "4",
"Encrypted": false,
"Endpoint": {
    "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
    "Port": 5439
},

```



```

"EnhancedVpcRouting": false,
"ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
"ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
"HsmStatus": {
  "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
  "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
  "Status": "applying"
},
"IamRoles": [
  {
    "ApplyStatus": "in-sync",
    "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
  }
],
"KmsKeyId": "kmsKeyId",
"LoggingStatus": {
  "BucketName": "amzn-s3-demo-bucket",
  "LastFailureMessage": "test message",
  "LastFailureTime": "2020-08-09T13:00:00.000Z",
  "LastSuccessfulDeliveryTime": "2020-08-08T13:00:00.000Z",
  "LoggingEnabled": true,
  "S3KeyPrefix": "/"
},
"MaintenanceTrackName": "current",
"ManualSnapshotRetentionPeriod": -1,
"MasterUsername": "awsuser",
"NextMaintenanceWindowStartTime": "2020-08-09T13:00:00.000Z",
"NodeType": "dc2.large",
"NumberOfNodes": 2,
"PendingActions": [],
"PendingModifiedValues": {
  "AutomatedSnapshotRetentionPeriod": 0,
  "ClusterIdentifier": "clusterIdentifier",
  "ClusterType": "clusterType",
  "ClusterVersion": "clusterVersion",
  "EncryptionType": "None",
  "EnhancedVpcRouting": false,
  "MaintenanceTrackName": "maintenanceTrackName",
  "MasterUserPassword": "masterUserPassword",
  "NodeType": "dc2.large",
  "NumberOfNodes": 1,
  "PubliclyAccessible": true
},
"PreferredMaintenanceWindow": "sun:13:00-sun:13:30",

```

```

    "PubliclyAccessible": true,
    "ResizeInfo": {
      "AllowCancelResize": true,
      "ResizeType": "ClassicResize"
    },
    "RestoreStatus": {
      "CurrentRestoreRateInMegaBytesPerSecond": 15,
      "ElapsedTimeInSeconds": 120,
      "EstimatedTimeToCompletionInSeconds": 100,
      "ProgressInMegaBytes": 10,
      "SnapshotSizeInMegaBytes": 1500,
      "Status": "restoring"
    },
    "SnapshotScheduleIdentifier": "snapshotScheduleIdentifier",
    "SnapshotScheduleState": "ACTIVE",
    "VpcId": "vpc-example",
    "VpcSecurityGroups": [
      {
        "Status": "active",
        "VpcSecurityGroupId": "sg-example"
      }
    ]
  }
}

```

Recursos de AwsRoute53 en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsRoute53 los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsRoute53HostedZone

El objeto AwsRoute53HostedZone proporciona información acerca de una zona alojada de Amazon Route 53, incluidos los cuatro servidores de nombres asignados a la zona alojada. Una zona alojada representa un conjunto de registros que se pueden administrar juntos y que pertenecen a un único nombre de dominio principal.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del AwsRoute53HostedZone objeto. Para ver las descripciones de AwsRoute53HostedZone los atributos, consulta [AwsRoute53 HostedZoneDetails](#) en la Referencia de la AWS Security Hub API.

Ejemplo

```
"AwsRoute53HostedZone": {
  "HostedZone": {
    "Id": "Z06419652JEMG09TA2XKL",
    "Name": "asff.testing",
    "Config": {
      "Comment": "This is an example comment."
    }
  },
  "NameServers": [
    "ns-470.awsdns-32.net",
    "ns-1220.awsdns-12.org",
    "ns-205.awsdns-13.com",
    "ns-1960.awsdns-51.co.uk"
  ],
  "QueryLoggingConfig": {
    "CloudWatchLogsLogGroupArn": {
      "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-group:asfftesting:*",
      "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "HostedZoneId": "Z00932193AF5H180PPNZD"
    }
  },
  "Vpcs": [
    {
      "Id": "vpc-05d7c6e36bc03ea76",
      "Region": "us-east-1"
    }
  ]
}
```

Recursos de AwsS3 en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsS3 los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsS3AccessPoint

AwsS3AccessPoint proporciona información acerca de un punto de acceso de Amazon S3. Los puntos de acceso de S3 son puntos de conexión de red con nombre que están asociados a los buckets que se pueden utilizar para llevar a cabo operaciones con objetos de S3.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del *AwsS3AccessPoint* objeto. Para ver las descripciones de *AwsS3AccessPoint* los atributos, consulte [AWSS3 AccessPointDetails](#) en la referencia de la AWS Security Hub API.

Ejemplo

```
"AwsS3AccessPoint": {
  "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-point",
  "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
  "Bucket": "amzn-s3-demo-bucket",
  "BucketAccountId": "123456789012",
  "Name": "asff-access-point",
  "NetworkOrigin": "VPC",
  "PublicAccessBlockConfiguration": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": true,
    "RestrictPublicBuckets": true
  },
  "VpcConfiguration": {
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
  }
}
```

AwsS3AccountPublicAccessBlock

AwsS3AccountPublicAccessBlock proporciona información sobre la configuración del bloque de acceso público de Amazon S3 para las cuentas.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del *AwsS3AccountPublicAccessBlock* objeto. Para ver las descripciones de *AwsS3AccountPublicAccessBlock* los atributos, consulte [AWSS3 AccountPublicAccessBlockDetails](#) en la referencia de la AWS Security Hub API.

Ejemplo

```
"AwsS3AccountPublicAccessBlock": {
  "BlockPublicAcls": true,
  "BlockPublicPolicy": true,
  "IgnorePublicAcls": false,
  "RestrictPublicBuckets": true
}
```

AwsS3Bucket

El objeto `AwsS3Bucket` proporciona información detallada sobre un bucket de Amazon S3.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsS3Bucket` objeto. Para ver las descripciones de *AwsS3Bucket* los atributos, consulte [AWSS3BucketDetails](#) en la referencia de la AWS Security Hub API.

Ejemplo

```
"AwsS3Bucket": {
  "AccessControlList": "{\\"grantSet\\":null,\\"grantList\\":[{\\"grantee\\":{\\"id\\":\\"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\\",\\"displayName\\":null},\\"permission\\":\\"FullControl\\"},{\\"grantee\\":\\"AllUsers\\",\\"permission\\":\\"ReadAcp\\"},{\\"grantee\\":\\"AuthenticatedUsers\\",\\"permission\\":\\"ReadAcp\\"}],",
  "BucketLifecycleConfiguration": {
    "Rules": [
      {
        "AbortIncompleteMultipartUpload": {
          "DaysAfterInitiation": 5
        },
        "ExpirationDate": "2021-11-10T00:00:00.000Z",
        "ExpirationInDays": 365,
        "ExpiredObjectDeleteMarker": false,
        "Filter": {
          "Predicate": {
            "Operands": [
              {
                "Prefix": "tmp/",
                "Type": "LifecyclePrefixPredicate"
              },
              {
                "Tag": {
                  "Key": "ArchiveAge",
                  "Value": "9m"
                }
              }
            ]
          }
        }
      }
    ]
  }
}
```

```

        "Type": "LifecycleTagPredicate"
      }
    ],
    "Type": "LifecycleAndOperator"
  }
},
"ID": "Move rotated logs to Glacier",
"NoncurrentVersionExpirationInDays": -1,
"NoncurrentVersionTransitions": [
  {
    "Days": 2,
    "StorageClass": "GLACIER"
  }
],
"Prefix": "rotated/",
"Status": "Enabled",
"Transitions": [
  {
    "Date": "2020-11-10T00:00:00.000Z",
    "Days": 100,
    "StorageClass": "GLACIER"
  }
]
}
]
},
"BucketLoggingConfiguration": {
  "DestinationBucketName": "s3serversideloggingbucket-123456789012",
  "LogFilePrefix": "buckettestreadwrite23435/"
},
"BucketName": "amzn-s3-demo-bucket",
"BucketNotificationConfiguration": {
  "Configurations": [{
    "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
    "Events": [
      "s3:ObjectCreated:Put"
    ]
  },
  "Filter": {
    "S3KeyFilter": {
      "FilterRules": [
        {
          "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
          "Value": "pre"
        }
      ]
    }
  }
},

```

```

    {
      "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
      "Value": "suf"
    },
  ]
}
},
"Type": "LambdaConfiguration"
}]
},
"BucketVersioningConfiguration": {
  "IsMfaDeleteEnabled": true,
  "Status": "Off"
},
"BucketWebsiteConfiguration": {
  "ErrorDocument": "error.html",
  "IndexDocumentSuffix": "index.html",
  "RedirectAllRequestsTo": {
    "HostName": "example.com",
    "Protocol": "http"
  },
},
"RoutingRules": [{
  "Condition": {
    "HttpErrorCodeReturnedEquals": "Redirected",
    "KeyPrefixEquals": "index"
  },
  "Redirect": {
    "HostName": "example.com",
    "HttpRedirectCode": "401",
    "Protocol": "HTTP",
    "ReplaceKeyPrefixWith": "string",
    "ReplaceKeyWith": "string"
  }
}]
},
"CreatedAt": "2007-11-30T01:46:56.000Z",
"ObjectLockConfiguration": {
  "ObjectLockEnabled": "Enabled",
  "Rule": {
    "DefaultRetention": {
      "Days": null,
      "Mode": "GOVERNANCE",
      "Years": 12
    }
  },
},

```

```

    },
  },
  "OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
  "OwnerName": "s3bucketowner",
  "PublicAccessBlockConfiguration": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": true,
    "RestrictPublicBuckets": true,
  },
  "ServerSideEncryptionConfiguration": {
    "Rules": [
      {
        "ApplyServerSideEncryptionByDefault": {
          "SSEAlgorithm": "AES256",
          "KMSEMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
        }
      }
    ]
  }
}

```

AwsS3Object

El objeto `AwsS3Object` proporciona información sobre un objeto de Amazon S3.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsS3Object` objeto. Para ver las descripciones de *AwsS3Object* los atributos, consulte [AWSS3ObjectDetails](#) en la referencia de la AWS Security Hub API.

Ejemplo

```

"AwsS3Object": {
  "ContentType": "text/html",
  "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
  "LastModified": "2012-04-23T18:25:43.511Z",
  "ServerSideEncryption": "aws:kms",
  "SSEKMSKeyId": "arn:aws:kms:us-west-2:123456789012:key/4dff8393-e225-4793-a9a0-608ec069e5a7",
  "VersionId": "ws310urg00jH_HH1lIxPE35P.MELYaYh"
}

```


Recursos de AwsSageMaker en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsSageMaker los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsSageMakerNotebookInstance

El `AwsSageMakerNotebookInstance` objeto proporciona información sobre una instancia de Amazon SageMaker AI notebook, que es una instancia de computación de aprendizaje automático que ejecuta la aplicación Jupyter Notebook.

En el siguiente ejemplo, se muestra el formato AWS de búsqueda de seguridad (ASFF) del objeto. `AwsSageMakerNotebookInstance` Para ver las descripciones de los atributos `AwsSageMakerNotebookInstance`, consulte [AwsSageMakerNotebookInstanceDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsSageMakerNotebookInstance": {
  "DirectInternetAccess": "Disabled",
  "InstanceMetadataServiceConfiguration": {
    "MinimumInstanceMetadataServiceVersion": "1",
  },
  "InstanceType": "ml.t2.medium",
  "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
  "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
  "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
  "NotebookInstanceName":
  "SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
  "NotebookInstanceStatus": "InService",
  "PlatformIdentifier": "notebook-all-v1",
  "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-SageMakerCustomExecution-1R0X32HGC38IW",
  "RootAccess": "Disabled",
  "SecurityGroups": [
    "sg-06b347359ab068745"
  ],
  "SubnetId": "subnet-02c0deea5fa64578e",
```

```
"Url":  
  "sagemakernotebookinstancerootaccessdisabledcompla-8myjcyofzixm.notebook.us-  
east-1.sagemaker.aws",  
  "VolumeSizeInGB": 5  
}
```

Recursos de AwsSecretsManager en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsSecretsManager los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsSecretsManagerSecret

El objeto AwsSecretsManagerSecret proporciona detalles sobre un secreto de Secrets Manager.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del AwsSecretsManagerSecret objeto. Para ver las descripciones de los atributos AwsSecretsManagerSecret, consulte [AwsSecretsManagerSecretDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsSecretsManagerSecret": {  
  "RotationRules": {  
    "AutomaticallyAfterDays": 30  
  },  
  "RotationOccurredWithinFrequency": true,  
  "KmsKeyId": "kmsKeyId",  
  "RotationEnabled": true,  
  "RotationLambdaArn": "arn:aws:lambda:us-  
west-2:777788889999:function:MyTestRotationLambda",  
  "Deleted": false,  
  "Name": "MyTestDatabaseSecret",  
  "Description": "My test database secret"  
}
```

Recursos de AwsSns en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los AwsSns recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsSnsTopic

El objeto AwsSnsTopic contiene detalles sobre un tema de Amazon Simple Notification Service.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del AwsSnsTopic objeto. Para ver las descripciones de los atributos AwsSnsTopic, consulte [AwsSnsTopicDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsSnsTopic": {
  "ApplicationSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
ApplicationSuccessFeedbackRoleArn",
  "FirehoseFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseFailureFeedbackRoleArn",
  "FirehoseSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseSuccessFeedbackRoleArn",
  "HttpFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpFailureFeedbackRoleArn",
  "HttpSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpSuccessFeedbackRoleArn",
  "KmsMasterKeyId": "alias/ExampleAlias",
  "Owner": "123456789012",
  "SqsFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsFailureFeedbackRoleArn",
  "SqsSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsSuccessFeedbackRoleArn",
  "Subscription": {
    "Endpoint": "http://sampleendpoint.com",
    "Protocol": "http"
  },
  "TopicName": "SampleTopic"
}
```

Recursos de AwsSqs en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los AwsSqs recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsSqsQueue

El objeto AwsSqsQueue contiene información acerca de una cola de Amazon Simple Queue Service.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del AwsSqsQueue objeto. Para ver las descripciones de los atributos AwsSqsQueue, consulte [AwsSqsQueueDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsSqsQueue": {  
  "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",  
  "KmsDataKeyReusePeriodSeconds": 60,,  
  "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",  
  "QueueName": "sample-queue"  
}
```

Recursos de AwsSsm en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para los AwsSsm recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsSsmPatchCompliance

El objeto AwsSsmPatchCompliance proporciona información sobre el estado de un parche en una instancia en función de la línea de base de revisiones que se utilizó para parchear la instancia.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del AwsSsmPatchCompliance objeto. Para ver las descripciones de los atributos AwsSsmPatchCompliance, consulte [AwsSsmPatchComplianceDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsSsmPatchCompliance": {
  "Patch": {
    "ComplianceSummary": {
      "ComplianceType": "Patch",
      "CompliantCriticalCount": 0,
      "CompliantHighCount": 0,
      "CompliantInformationalCount": 0,
      "CompliantLowCount": 0,
      "CompliantMediumCount": 0,
      "CompliantUnspecifiedCount": 461,
      "ExecutionType": "Command",
      "NonCompliantCriticalCount": 0,
      "NonCompliantHighCount": 0,
      "NonCompliantInformationalCount": 0,
      "NonCompliantLowCount": 0,
      "NonCompliantMediumCount": 0,
      "NonCompliantUnspecifiedCount": 0,
      "OverallSeverity": "UNSPECIFIED",
      "PatchBaselineId": "pb-0c5b2769ef7cbe587",
      "PatchGroup": "ExamplePatchGroup",
      "Status": "COMPLIANT"
    }
  }
}
```

Recursos de AwsStepFunctions en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para `AwsStepFunctions` los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsStepFunctionStateMachine

El objeto `AwsStepFunctionStateMachine` proporciona información sobre una máquina de estados de AWS Step Functions, que es un flujo de trabajo que consta de una serie de pasos basados en eventos.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsStepFunctionStateMachine` objeto. Para ver las descripciones de los atributos

AwsStepFunctionStateMachine, consulte [AwsStepFunctionStateMachine](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsStepFunctionStateMachine": {
  "StateMachineArn": "arn:aws:states:us-east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
  "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
  "Status": "ACTIVE",
  "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-StatesExecutionRole-1PNM71RV01UKT",
  "Type": "STANDARD",
  "LoggingConfiguration": {
    "Level": "OFF",
    "IncludeExecutionData": false
  },
  "TracingConfiguration": {
    "Enabled": false
  }
}
```

Recursos de AwsWaf en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsWaf los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsWafRateBasedRule

El objeto `AwsWafRateBasedRule` contiene detalles sobre una regla basada en tasas de AWS WAF para los recursos globales. Una regla AWS WAF basada en tasas proporciona ajustes para indicar cuándo permitir, bloquear o contar una solicitud. Las regla basada en tasas incluyen la cantidad de solicitudes que llegan durante un período de tiempo específico.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsWafRateBasedRule` objeto. Para ver las descripciones de los atributos `AwsWafRateBasedRule`, consulte [AwsWafRateBasedRuleDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafRateBasedRule":{
  "MatchPredicates" : [{
    "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
    "Negated" : "True",
    "Type" : "IPMatch" ,
  }],
  "MetricName" : "MetricName",
  "Name" : "Test",
  "RateKey" : "IP",
  "RateLimit" : 235000,
  "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRateBasedRule

El objeto `AwsWafRegionalRateBasedRule` contiene detalles sobre una regla basada en tasas para los recursos Regionales. Una regla basada en tasas proporciona configuraciones para indicar cuándo permitir, bloquear o contar una solicitud. Las regla basada en tasas incluyen la cantidad de solicitudes que llegan durante un período de tiempo específico.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsWafRegionalRateBasedRule` objeto. Para ver las descripciones de los atributos `AwsWafRegionalRateBasedRule`, consulte [AwsWafRegionalRateBasedRuleDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafRegionalRateBasedRule":{
  "MatchPredicates" : [{
    "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
    "Negated" : "True",
    "Type" : "IPMatch" ,
  }],
  "MetricName" : "MetricName",
  "Name" : "Test",
  "RateKey" : "IP",
  "RateLimit" : 235000,
  "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRule

El `AwsWafRegionalRule` objeto proporciona detalles sobre una regla AWS WAF regional. Esta regla identifica las solicitudes web que desea permitir, bloquear o contar.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsWafRegionalRule` objeto. Para ver las descripciones de los atributos `AwsWafRegionalRule`, consulte [AwsWafRegionalRuleDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafRegionalRule": {
  "MetricName": "SampleWAF_Rule__Metric_1",
  "Name": "bb-waf-regional-rule-not-empty-conditions-compliant",
  "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de95fe",
  "PredicateList": [{
    "DataId": "127d9346-e607-4e93-9286-c1296fb5445a",
    "Negated": false,
    "Type": "GeoMatch"
  }]
}
```

AwsWafRegionalRuleGroup

El objeto `AwsWafRegionalRuleGroup` proporciona detalles sobre un grupo de reglas Regionales de AWS WAF . Un grupo de reglas es una colección de reglas predefinidas que agrega a una lista de control de acceso web (ACL web).

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsWafRegionalRuleGroup` objeto. Para ver las descripciones de los atributos `AwsWafRegionalRuleGroup`, consulte [AwsWafRegionalRuleGroupDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafRegionalRuleGroup": {
  "MetricName": "SampleWAF_Metric_1",
  "Name": "bb-WAFClassicRuleGroupWithRuleCompliant",
  "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
  "Rules": [{
    "Action": {
      "Type": "ALLOW"
    }
  ]
}
```



```

    }
  ],
  "Priority": 1,
  "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
  "Type": "REGULAR"
}

```

AwsWafRegionalWebAcl

`AwsWafRegionalWebAcl` proporciona detalles sobre una lista AWS WAF regional de control de acceso a la web (ACL web). Una ACL web contiene las reglas que identifican las solicitudes que desea permitir, bloquear o contar.

A continuación, se muestra un ejemplo de resultado de `AwsWafRegionalWebAcl` en Formato de resultados de seguridad de AWS (ASFF). Para ver las descripciones de los atributos `AwsApiGatewayV2Stage`, consulte [AwsWafRegionalWebAclDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```

"AwsWafRegionalWebAcl": {
  "DefaultAction": "ALLOW",
  "MetricName" : "web-regional-webacl-metric-1",
  "Name": "WebACL_123",
  "RulesList": [
    {
      "Action": {
        "Type": "Block"
      },
      "Priority": 3,
      "RuleId": "24445857-852b-4d47-bd9c-61f05e4d223c",
      "Type": "REGULAR",
      "ExcludedRules": [
        {
          "ExclusionType": "Exclusion",
          "RuleId": "Rule_id_1"
        }
      ],
      "OverrideAction": {
        "Type": "OVERRIDE"
      }
    }
  ]
}

```

```
  ],
  "WebAclId": "443c76f4-2e72-4c89-a2ee-389d501c1f67"
}
```

AwsWafRule

`AwsWafRule` proporciona información sobre una AWS WAF regla. Una AWS WAF regla identifica las solicitudes web que desea permitir, bloquear o contar.

El siguiente es un ejemplo de `AwsWafRule` búsqueda en el formato AWS de búsqueda de seguridad (ASFF). Para ver las descripciones de los atributos `AwsApiGatewayV2Stage`, consulte [AwsWafRuleDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafRule": {
  "MetricName": "AwsWafRule_Metric_1",
  "Name": "AwsWafRule_Name_1",
  "PredicateList": [{
    "DataId": "cdd225da-32cf-4773-1dc2-3bca3ed9c19c",
    "Negated": false,
    "Type": "GeoMatch"
  }],
  "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de953e"
}
```

AwsWafRuleGroup

`AwsWafRuleGroup` proporciona información sobre un grupo de AWS WAF reglas. Un grupo de reglas de AWS WAF es un conjunto de reglas predefinidas que agrega a una lista de control de acceso web (ACL web).

A continuación se muestra un ejemplo de `AwsWafRuleGroup` hallazgo en el formato de búsqueda de AWS seguridad (ASFF). Para ver las descripciones de los atributos `AwsApiGatewayV2Stage`, consulte [AwsWafRuleGroupDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafRuleGroup": {
  "MetricName": "SampleWAF_Metric_1",
  "Name": "bb-WAFRuleGroupWithRuleCompliant",
  "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
}
```

```

    "Rules": [{
      "Action": {
        "Type": "ALLOW",
      },
      "Priority": 1,
      "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
      "Type": "REGULAR"
    }]
  }

```

AwsWafv2RuleGroup

El `AwsWafv2RuleGroup` objeto proporciona detalles sobre un grupo de reglas AWS WAF V2.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del `AwsWafv2RuleGroup` objeto. Para ver las descripciones de `AwsWafv2RuleGroup` los atributos, consulta el apartado [AwsWafv2](#) de RuleGroupDetails la referencia de la AWS Security Hub API.

Ejemplo

```

"AwsWafv2RuleGroup": {
  "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Capacity": 1000,
  "Description": "Resource for ASFF",
  "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Name": "wafv2rulegroupasff",
  "Rules": [{
    "Action": {
      "Allow": {
        "CustomRequestHandling": {
          "InsertHeaders": [
            {
              "Name": "AllowActionHeader1Name",
              "Value": "AllowActionHeader1Value"
            },
            {
              "Name": "AllowActionHeader2Name",
              "Value": "AllowActionHeader2Value"
            }
          ]
        }
      }
    }
  ]
},

```

```
"Name": "RuleOne",
"Priority": 1,
"VisibilityConfig": {
  "CloudWatchMetricsEnabled": true,
  "MetricName": "rulegroupasff",
  "SampledRequestsEnabled": false
}
}],
"VisibilityConfig": {
  "CloudWatchMetricsEnabled": true,
  "MetricName": "rulegroupasff",
  "SampledRequestsEnabled": false
}
}
```

AwsWafWebAcl

El `AwsWafWebAcl` objeto proporciona detalles sobre una ACL AWS WAF web.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsWafWebAcl` objeto. Para ver las descripciones de los atributos `AwsWafWebAcl`, consulte [AwsWafWebAclDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsWafWebAcl": {
  "DefaultAction": "ALLOW",
  "Name": "MyWafAcl",
  "Rules": [
    {
      "Action": {
        "Type": "ALLOW"
      },
      "ExcludedRules": [
        {
          "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"
        }
      ],
      "OverrideAction": {
        "Type": "NONE"
      },
      "Priority": 1,
      "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98",
    }
  ]
}
```

```

        "Type": "REGULAR"
    }
],
    "WebAclId": "waf-1234567890"
}

```

AwsWafv2WebAcl

El `AwsWafv2WebAcl` objeto proporciona detalles sobre una ACL web AWS WAF V2.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsWafv2WebAcl` objeto. Para ver las descripciones de `AwsWafv2WebAcl` los atributos, consulta el apartado [AwsWafv2](#) de `WebAclDetails` la referencia de la AWS Security Hub API.

Ejemplo

```

"AwsWafv2WebAcl": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1326,
    "CaptchaConfig": {
        "ImmunityTimeProperty": {
            "ImmunityTime": 500
        }
    },
    "DefaultAction": {
        "Block": {}
    },
    "Description": "Web ACL for JsonBody testing",
    "ManagedbyFirewallManager": false,
    "Name": "WebACL-RoaD4QexqSxG",
    "Rules": [{
        "Action": {
            "RuleAction": {
                "Block": {}
            }
        },
        "Name": "TestJsonBodyRule",
        "Priority": 1,
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "JsonBodyMatchMetric"
        }
    }]
}

```

```
}
}],
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "TestingJsonBodyMetric"
}
}
```

Recursos de AwsXray en el ASFF

A continuación se muestran ejemplos de la sintaxis del formato de búsqueda de AWS seguridad (ASFF) para AwsXray los recursos.

AWS Security Hub normaliza los hallazgos de diversas fuentes en ASFF. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

AwsXrayEncryptionConfig

El AwsXrayEncryptionConfig objeto contiene información sobre la configuración de cifrado de AWS X-Ray.

En el siguiente ejemplo, se muestra el formato de búsqueda de AWS seguridad (ASFF) del AwsXrayEncryptionConfig objeto. Para ver las descripciones de los atributos AwsXrayEncryptionConfig, consulte [AwsXrayEncryptionConfigDetails](#) en la referencia de la API de AWS Security Hub .

Ejemplo

```
"AwsXRayEncryptionConfig":{
  "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
  "Status": "UPDATING",
  "Type": "KMS"
}
```

Objeto Container del ASFF

El siguiente ejemplo muestra la sintaxis del formato de búsqueda de AWS seguridad (ASFF) del Container objeto. Para ver las descripciones de los atributos Container, consulte [ContainerDetails](#) en la referencia de la API de AWS Security Hub . Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

Ejemplo

```
"Container": {
  "ContainerRuntime": "docker",
  "ImageId": "image12",
  "ImageName": "1111111/knotejs@sha256:372131c9fef1111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "Name": "knote",
  "Privileged": true,
  "VolumeMounts": [{
    "Name": "vol-03909e9",
    "MountPath": "/mnt/etc"
  }]
}
```

Objeto Other del ASFF

El siguiente ejemplo muestra la sintaxis del formato de búsqueda de AWS seguridad (ASFF) del `Other` objeto. Para obtener información general sobre el ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

El objeto `Other` le permite proporcionar campos y valores personalizados. Utilice el objeto `Other` en los siguientes casos.

- El tipo de recurso no tiene el objeto `Details` correspondiente. Para proporcionar detalles sobre el recurso, utilice el objeto `Other`.
- El objeto `Details` del tipo de recurso no incluye todos los atributos que desea rellenar. En este caso, use el objeto `Details` de detalles del tipo de recurso para rellenar los atributos disponibles. Utilice el objeto `Other` para rellenar los atributos que no están en el objeto específico del tipo.
- El tipo de recurso no es uno de los tipos proporcionados. En este caso, `Other` se establece en `Resource.Type` y se usa el objeto `Other` para rellenar los detalles.

Tipo: mapa de hasta 50 pares clave-valor

Cada par clave-valor debe cumplir los siguientes requisitos.

- La clave debe tener menos de 128 caracteres.
- El valor debe tener menos de 1024 caracteres.

Visualización de información en Security Hub CSPM

En AWS Security Hub Cloud Security Posture Management (CSPM), una visión es una colección de hallazgos relacionados. La información puede identificar un área de seguridad específica que requiera atención e intervención. Por ejemplo, una información podría señalar EC2 casos objeto de hallazgos que detecten prácticas de seguridad inadecuadas. Una información reúne los resultados de todos los proveedores de resultados.

Cada información se define mediante una instrucción GROUP BY y filtros opcionales. La instrucción GROUP BY indica cómo agrupar los resultados coincidentes e identifica el tipo de elemento al que se aplica la información. Por ejemplo, si una información se agrupa por identificador de recurso, la información genera una lista de identificadores de recursos. Los filtros opcionales reducen los resultados coincidentes para la información. Por ejemplo, es posible que solo desee ver resultados de proveedores específicos o resultados que estén relacionados con tipos específicos de recursos.

Security Hub CSPM ofrece varios conocimientos gestionados integrados. No puede modificar ni eliminar la información administrada. Para realizar un seguimiento de los problemas de seguridad que son exclusivos de su AWS entorno y uso, puede crear información personalizada.

La página de información de la consola AWS Security Hub Cloud Security Posture Management (CSPM) muestra la lista de información disponible.

De forma predeterminada, la lista muestra tanto los hallazgos gestionados como los personalizados. Para filtrar la lista de información en función del tipo de hallazgos, elija el tipo en el menú desplegable que se encuentra junto al campo de filtro.

- Para mostrar todos los hallazgos disponibles, seleccione Todos los hallazgos. Esta es la opción predeterminada.
- Para mostrar solo los conocimientos gestionados, elija los conocimientos gestionados por Security Hub CSPM.
- Para mostrar solo información personalizada, elija Hallazgos personalizados.

También puede filtrar la lista de información en función del nombre de cada una. Para hacerlo, en el campo de filtro, escriba el texto que se utilizará para filtrar la lista. El filtro no distingue entre mayúsculas y minúsculas. El filtro busca hallazgos que contengan el texto en cualquier parte del nombre.

Una información solo devuelve resultados si ha habilitado integraciones o estándares que produzcan resultados coincidentes. Por ejemplo, la información administrada 29. Principales recursos por número de comprobaciones CIS no superadas solo devuelve resultados si habilita una versión del estándar del Indicador de referencia de AWS de Center for Internet Security (CIS).

Revisión de los conocimientos del Security Hub (CSPM) y adopción de medidas en función de ellos

Para cada información, AWS Security Hub Cloud Security Posture Management (CSPM) determina primero las conclusiones que coinciden con los criterios del filtro y, a continuación, utiliza el atributo de agrupamiento para agrupar las conclusiones coincidentes.

Desde la página Información en la consola puede ver y tomar medidas sobre los resultados y los hallazgos.

Si habilita la agregación entre regiones, los resultados de la información administrada (cuando haya iniciado sesión en la región de agregación) incluirán los resultados de la región de agregación y de las regiones vinculadas. Los resultados de la información personalizada, si la información no se filtra por región, también incluyen los resultados de la región de agregación y las regiones vinculadas (cuando haya iniciado sesión en la región de agregación). En otras regiones, los resultados de la información son solo para esa región.

Para obtener más información acerca de la configuración de agregación entre regiones, consulte [Agregación de datos del CSPM en todas las regiones](#).

Visualización y adopción de medidas sobre los resultados de la información

Los resultados del conocimiento constan de una lista agrupada de los resultados del conocimiento. Por ejemplo, si la información se agrupa por identificadores de recursos, los resultados de la información son la lista de identificadores del recurso. Cada elemento de la lista de resultados indica el número de hallazgos coincidentes para ese elemento.

Si los resultados se agrupan por identificador de recurso o tipo de recurso, los resultados incluyen todos los recursos de los hallazgos correspondientes. Esto incluye los recursos que tienen un tipo diferente del tipo de recurso especificado en los criterios del filtro. Por ejemplo, un hallazgo identifica los resultados asociados a los buckets de S3. Si un resultado coincidente contiene un bucket de S3 y una clave de acceso de IAM, los resultados de información incluyen ambos recursos.

En la consola CSPM de Security Hub, la lista de resultados se ordena del mayor al menor número de hallazgos coincidentes. Security Hub CSPM solo puede mostrar 100 resultados. Si hay más de 100 valores de agrupamiento, solo verá los primeros 100.

Además de la lista de resultados, los resultados de conocimientos muestran un conjunto de gráficos que resume el número de hallazgos coincidentes para los siguientes atributos.

- Etiqueta de gravedad: número de resultados para cada etiqueta de gravedad
- Cuenta de AWS ID: los cinco principales representan IDs los resultados coincidentes
- Tipo de recurso: los cinco tipos de recursos principales para los resultados correspondientes
- ID del recurso: los cinco recursos principales IDs para encontrar los resultados coincidentes
- Nombre del producto: los cinco principales proveedores de hallazgos para los resultados correspondientes

Si ha configurado acciones personalizadas, puede enviar los resultados seleccionados a una acción personalizada. La acción debe estar asociada a una CloudWatch regla de Amazon para el tipo de Security Hub Insight Results evento. Para obtener más información, consulte [the section called “Respuesta y corrección automatizadas”](#). Si no ha configurado acciones personalizadas, el menú Acciones está desactivado.

Security Hub CSPM console

Para visualizar y adoptar medidas sobre los resultados de la información (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Insights.
3. Para mostrar la lista de resultados de conocimientos, elija el nombre del conocimiento.
4. Seleccione la casilla de verificación de cada resultado que desee enviar a la acción personalizada.
5. En el menú Actions (Acciones), elija la acción personalizada.

Security Hub CSPM API, AWS CLI

Para ver los resultados de la información y tomar medidas al respecto (API,) AWS CLI

Para ver los resultados de la información, utilice el [>GetInsightResults](#) funcionamiento de la API CSPM de Security Hub. Si usa el AWS CLI, ejecute el [get-insight-results](#) comando.

Para identificar la información para la que obtener resultados, necesita el ARN de la información. Para obtener información ARNs personalizada, utilice la operación de la [GetInsights](#) API o el [get-insight-results](#) comando.

En el siguiente ejemplo, se recuperan los resultados de la información especificada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Para obtener información acerca de cómo crear acciones personalizadas mediante programación, consulte [Utilizar acciones personalizadas para enviar las conclusiones y los resultados de información a EventBridge](#).

Para visualizar y tomar medidas sobre los hallazgos en los resultados de la información (consola)

Desde una lista de resultados de información en la consola CSPM de Security Hub, puede mostrar la lista de hallazgos de cada resultado.

Para visualizar y tomar medidas sobre los resultados de la información (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Insights.
3. Para mostrar la lista de resultados de conocimientos, elija el nombre del conocimiento.
4. Para mostrar la lista de hallazgos de un resultado de conocimiento, elija el elemento de la lista de resultados. La lista de hallazgos muestra los hallazgos activos del resultado de conocimiento seleccionado que tienen un estado de flujo de trabajo NEW o NOTIFIED.

En la lista de resultados puede realizar las siguientes acciones:

- [Filtrado de resultados en Security Hub \(CSPM\)](#)

- [Revisión de los detalles y el historial de resultados](#)
- [Configuración del estado del flujo de trabajo de los hallazgos en Security Hub \(CSPM\)](#)
- [Enviar los resultados a un Security Hub \(CSPM\) personalizado \(acción\)](#)

Información gestionada en Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (CSPM) proporciona varios conocimientos gestionados.

No puede editar ni eliminar los conocimientos gestionados por CSPM de Security Hub. Puede [ver y tomar medidas sobre los resultados y hallazgos de conocimientos](#). También puede [utilizar conocimientos administrados como base para un nuevo conocimiento personalizado](#).

Al igual que con todos los conocimientos, un conocimiento administrado solo devuelve resultados si ha habilitado integraciones de productos o estándares de seguridad que pueden producir hallazgos coincidentes.

En el caso de los hallazgos agrupados en base al identificador de recursos, los resultados incluyen los identificadores de todos los recursos en los elementos que coinciden con los parámetros. Aquí se incluyen los recursos que poseen un tipo diferente al tipo de recurso que se indica en los criterios del filtro. Por ejemplo, el hallazgo 2 en la siguiente lista identifica los resultados asociados a los buckets de Amazon S3. Si un resultado coincidente contiene un bucket de S3 y una clave de acceso de IAM, los resultados de información incluyen ambos recursos.

Security Hub CSPM ofrece actualmente los siguientes conocimientos gestionados:

1. AWS recursos con la mayoría de los hallazgos

ARN: `arn:aws:securityhub:::insight/securityhub/default/1`

Agrupados por: identificador de recursos

Filtros de resultados:

- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

2. Buckets de S3 con permisos de lectura o escritura públicos

ARN: `arn:aws:securityhub:::insight/securityhub/default/10`

Agrupados por: identificador de recursos

Filtros de resultados:

- El tipo comienza con Effects/Data Exposure
- El tipo de recurso es AwsS3Bucket
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

3. AMLs que están generando la mayoría de los hallazgos

ARN: `arn:aws:securityhub:::insight/securityhub/default/3`

Agrupados por: ID de imagen de EC2 instancia

Filtros de resultados:

- El tipo de recurso es AwsEc2Instance
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

4. EC2 instancias involucradas en tácticas, técnicas y procedimientos conocidos (TTPs)

ARN: `arn:aws:securityhub:::insight/securityhub/default/14`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con TTPs
- El tipo de recurso es AwsEc2Instance
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

5. AWS directores con actividad sospechosa en las claves de acceso

ARN: `arn:aws:securityhub:::insight/securityhub/default/9`

Agrupados por: nombre de entidad principal de la clave de acceso de IAM

Filtros de resultados:

- El tipo de recurso es `AwsIamAccessKey`
- El estado de registro es `ACTIVE`
- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

6. AWS instancias de recursos que no cumplen con los estándares o las mejores prácticas de seguridad

ARN: `arn:aws:securityhub:::insight/securityhub/default/6`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo es `Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices`
- El estado de registro es `ACTIVE`
- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

7. AWS recursos asociados a la posible exfiltración de datos

ARN: `arn:aws:securityhub:::insight/securityhub/default/7`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con `Exfiltración/ Effects/Data`
- El estado de registro es `ACTIVE`
- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

8. AWS recursos asociados al consumo no autorizado de recursos

ARN: `arn:aws:securityhub:::insight/securityhub/default/8`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con `Effects/Resource Consumption`
- El estado de registro es `ACTIVE`
- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

9. Buckets de S3 que no cumplen los estándares o las prácticas recomendadas de seguridad

ARN: `arn:aws:securityhub:::insight/securityhub/default/11`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo de recurso es `AwsS3Bucket`
- El tipo es `Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices`
- El estado de registro es `ACTIVE`
- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

10. Buckets de S3 con información confidencial

ARN: `arn:aws:securityhub:::insight/securityhub/default/12`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo de recurso es `AwsS3Bucket`
- El tipo comienza con `Sensitive Data Identifications/`
- El estado de registro es `ACTIVE`
- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

11. Credenciales que podrían haberse filtrado

ARN: `arn:aws:securityhub:::insight/securityhub/default/13`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con `Sensitive Data Identifications/Passwords/`
- El estado de registro es `ACTIVE`
- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

12. EC2 instancias a las que les faltan parches de seguridad debido a vulnerabilidades importantes

ARN: `arn:aws:securityhub:::insight/securityhub/default/16`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con Software and Configuration Checks/Vulnerabilities/CVE
- El tipo de recurso es AwsEc2Instance
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

13. EC2 casos con un comportamiento inusual general

ARN: `arn:aws:securityhub:::insight/securityhub/default/17`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con Unusual Behaviors
- El tipo de recurso es AwsEc2Instance
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

14. EC2 instancias que tienen puertos accesibles desde Internet

ARN: `arn:aws:securityhub:::insight/securityhub/default/18`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con Software and Configuration Checks/AWS Security Best Practices/Network Reachability
- El tipo de recurso es AwsEc2Instance
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

15. EC2 instancias que no cumplen con los estándares o las mejores prácticas de seguridad

ARN: `arn:aws:securityhub:::insight/securityhub/default/19`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con una de las siguientes opciones:
 - Software and Configuration Checks/Industry and Regulatory Standards/
 - Software and Configuration Checks/AWS Security Best Practices
- El tipo de recurso es AwsEc2Instance
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

16. EC2 instancias que están abiertas a Internet

ARN: `arn:aws:securityhub:::insight/securityhub/default/21`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con Software and Configuration Checks/AWS Security Best Practices/Network Reachability
- El tipo de recurso es AwsEc2Instance
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

17. EC2 instancias asociadas con el reconocimiento del adversario

ARN: `arn:aws:securityhub:::insight/securityhub/default/22`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con /Discovery/Recon TTPs
- El tipo de recurso es AwsEc2Instance
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

18. AWS recursos asociados al malware

ARN: `arn:aws:securityhub:::insight/securityhub/default/23`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con una de las siguientes opciones:
 - Effects/Data Exfiltration/Trojan
 - TTPs/Initial Access/Trojan
 - TTPs/Command and Control/Backdoor
 - TTPs/Command and Control/Trojan
 - Software and Configuration Checks/Backdoor
 - Unusual Behaviors/VM/Backdoor
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

19. AWS recursos asociados a problemas de criptomonedas

ARN: `arn:aws:securityhub:::insight/securityhub/default/24`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con una de las siguientes opciones:
 - Effects/Resource Consumption/Cryptocurrency
 - TTPs/Command and Control/CryptoCurrency
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

20. AWS recursos con intentos de acceso no autorizados

ARN: `arn:aws:securityhub:::insight/securityhub/default/25`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con una de las siguientes opciones:
 - TTPs/Command and Control/UnauthorizedAccess
 - TTPs/Initial Access/UnauthorizedAccess
 - Effects/Data Exfiltration/UnauthorizedAccess

- Unusual Behaviors/User/UnauthorizedAccess
- Effects/Resource Consumption/UnauthorizedAccess
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

21. Indicadores de información de amenazas con la mayoría de coincidencias durante la semana pasada

ARN: `arn:aws:securityhub:::insight/securityhub/default/26`

Filtros de resultados:

- Creado en los últimos 7 días

22. Principales cuentas por número de hallazgos

ARN: `arn:aws:securityhub:::insight/securityhub/default/27`

Agrupados por: Cuenta de AWS ID

Filtros de resultados:

- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

23. Principales productos por número de hallazgos

ARN: `arn:aws:securityhub:::insight/securityhub/default/28`

Agrupados por: Nombre del producto

Filtros de resultados:

- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

24. Gravedad por número de hallazgos

ARN: `arn:aws:securityhub:::insight/securityhub/default/29`

Agrupados por: etiqueta de gravedad

Filtros de resultados:

- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

25. Principales buckets de S3 por número de hallazgos

ARN: `arn:aws:securityhub:::insight/securityhub/default/30`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo de recurso es `AwsS3Bucket`
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

26. EC2 Instancias principales por recuento de hallazgos

ARN: `arn:aws:securityhub:::insight/securityhub/default/31`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo de recurso es `AwsEc2Instance`
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

27. AMIs Encabezados por recuentos de hallazgos

ARN: `arn:aws:securityhub:::insight/securityhub/default/32`

Agrupados por: ID de imagen de la EC2 instancia

Filtros de resultados:

- El tipo de recurso es `AwsEc2Instance`
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

28. Principales usuarios de IAM por número de hallazgos

ARN: `arn:aws:securityhub:::insight/securityhub/default/33`

Agrupados por: ID de clave de acceso de IAM

Filtros de resultados:

- El tipo de recurso es `AwsIamAccessKey`
- El estado de registro es `ACTIVE`
- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

29. Principales recursos por número de comprobaciones CIS no superadas

ARN: `arn:aws:securityhub:::insight/securityhub/default/34`

Agrupados por: ID de recurso

Filtros de resultados:

- El ID del generador comienza con `arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule`
- Actualizado en el último día
- El estado de conformidad es `FAILED`
- El estado de registro es `ACTIVE`
- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

30. Principales integraciones por número de hallazgos

ARN: `arn:aws:securityhub:::insight/securityhub/default/35`

Agrupados por: ARN del producto

Filtros de resultados:

- El estado de registro es `ACTIVE`
- El estado de flujo de trabajo es `NEW` o `NOTIFIED`

31. Recursos con las comprobaciones de seguridad que más fallan

ARN: `arn:aws:securityhub:::insight/securityhub/default/36`

Agrupados por: ID de recurso

Filtros de resultados:

- Actualizado en el último día
- El estado de conformidad es FAILED
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

32. Usuarios de IAM con actividad sospechosa

ARN: `arn:aws:securityhub:::insight/securityhub/default/37`

Agrupados por: usuario de IAM

Filtros de resultados:

- El tipo de recurso es `AwsIamUser`
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

33. Recursos con la mayoría de los AWS Health hallazgos

ARN: `arn:aws:securityhub:::insight/securityhub/default/38`

Agrupados por: ID de recurso

Filtros de resultados:

- `ProductName` igual a `Health`

34. Recursos con la mayoría de los AWS Config hallazgos

ARN: `arn:aws:securityhub:::insight/securityhub/default/39`

Agrupados por: ID de recurso

Filtros de resultados:

- `ProductName` igual a `Config`

35. Aplicaciones con la mayor cantidad de resultados

ARN: `arn:aws:securityhub:::insight/securityhub/default/40`

Agrupado por: `ResourceApplicationArn`

Filtros de resultados:

- `RecordState` igual a `ACTIVE`
- `Workflow.Status` es igual a `NEW` o `NOTIFIED`

Descripción de la información personalizada en Security Hub (CSPM)

Además de la información gestionada por AWS Security Hub Cloud Security Posture Management (CSPM), puede crear información personalizada en Security Hub CSPM para realizar un seguimiento de los problemas específicos de su entorno. Los hallazgos personalizados le permiten realizar un seguimiento de un subconjunto de problemas seleccionados.

Estos son algunos ejemplos de hallazgos personalizados que puede resultar útil configurar:

- Si tiene una cuenta de administrador, puede configurar un hallazgo personalizado para hacer un seguimiento de los resultados críticos y de alta gravedad que estén afectando a las cuentas de los miembros.
- Si confía en un [AWS servicio integrado](#) específico, puede configurar una información personalizada para realizar un seguimiento de los hallazgos críticos y de alta gravedad de ese servicio.
- Si confía en una [integración de terceros](#), puede configurar un hallazgo personalizado para realizar un seguimiento de los hallazgos críticos y de alta gravedad de ese producto integrado.

Puede crear conocimientos personalizados completamente nuevos, o comenzar a partir de un conocimiento personalizado o administrado existente.

Cada hallazgo se puede configurar con las siguientes opciones:

- **Atributo de agrupación:** el atributo de agrupación determina los elementos que se muestran en la lista de resultados del hallazgo. Por ejemplo, si el atributo de agrupación es Nombre del producto, los resultados del hallazgo muestran el número de hallazgos asociados a cada proveedor.
- **Filtros opcionales:** Los filtros opcionales afinan la cantidad de resultados que coinciden con los parámetros del hallazgo.

Un hallazgo se incluye en los resultados de la información solo si coincide con todos los filtros proporcionados. Por ejemplo, si los filtros son «El nombre del producto es GuardDuty» y «el tipo de recurso es `AwsS3Bucket`», los resultados que coincidan deben cumplir ambos criterios.

Sin embargo, el CSPM de Security Hub aplica la lógica OR booleana a los filtros que utilizan el mismo atributo pero valores diferentes. Por ejemplo, si los filtros son «El nombre del producto es GuardDuty» y «El nombre del producto es Amazon Inspector», el resultado coincide si lo generó Amazon GuardDuty o Amazon Inspector.

Si utiliza el identificador de recurso o el tipo de recurso como atributo de agrupación, los resultados de la información incluirán todos los recursos incluidos en los resultados. La lista no se limita a los recursos que coinciden con un filtro de tipo de recurso. Por ejemplo, un hallazgo identifica los resultados asociados a los buckets de S3 y los agrupa por identificador de recursos. Un resultado coincidente contiene un recurso de bucket de S3 y un recurso de clave de acceso de IAM. Los resultados del hallazgo incluyen ambos recursos.

Si habilitó la [agregación entre regiones](#) y, luego, crea un hallazgo personalizado, el hallazgo se aplica a los resultados que coinciden con la región de agregación y las regiones vinculadas. La única excepción es que su información incluya un filtro de región.

Creación de hallazgos personalizados

En AWS Security Hub Cloud Security Posture Management (CSPM), se puede utilizar información personalizada para recopilar un conjunto específico de hallazgos y realizar un seguimiento de los problemas que son exclusivos de su entorno. Para obtener información general sobre hallazgos personalizados, consulte [Descripción de la información personalizada en Security Hub \(CSPM\)](#).

Elija el método que prefiera y siga los pasos para crear una información personalizada en Security Hub (CSPM).

Security Hub CSPM console

Para crear un hallazgo personalizado (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Hallazgos.
3. Seleccione Crear hallazgo.
4. Para seleccionar el atributo de agrupación para el conocimiento:
 - a. Seleccione el cuadro de búsqueda para ver las opciones de filtro.
 - b. Elija Group by (Agrupar por).

- c. Seleccione el atributo que se va a utilizar para agrupar los resultados asociados a este hallazgo.
- d. Seleccione Aplicar.
5. De manera opcional, elija los filtros adicionales que desee utilizar para este hallazgo. Para cada filtro, defina los criterios de filtro y, a continuación, elija Aplicar.
6. Seleccione Crear hallazgo.
7. Escriba un Nombre del hallazgo y elija Crear hallazgo.

Security Hub CSPM API

Para crear un hallazgo personalizado (API)

1. Para crear una información personalizada, utilice el [CreateInsight](#) funcionamiento de la API CSPM de Security Hub. Si usa el AWS CLI, ejecute el [create-insight](#) comando.
2. Rellene el parámetro Name con un nombre para su hallazgo personalizado.
3. Rellene el parámetro Filters para especificar qué resultados incluir en el hallazgo.
4. Rellene el parámetro GroupByAttribute para especificar qué atributo se utiliza para agrupar los resultados que se incluyen en el hallazgo.
5. Si lo desea, rellene el parámetro SortCriteria para ordenar los resultados por un campo específico.

En el siguiente ejemplo, se crea un hallazgo personalizado que incluye los resultados críticos con el tipo de recurso `AwsIamRole`. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (`\`) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub create-insight --name "Critical role findings" --filters
'{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole" }],
"SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

Para crear una información personalizada (PowerShell)

1. Utilice el cmdlet `New-SHUBInsight`.
2. Rellene el parámetro Name con un nombre para su hallazgo personalizado.

3. Rellene el parámetro `Filter` para especificar qué resultados incluir en el hallazgo.
4. Rellene el parámetro `GroupByAttribute` para especificar qué atributo se utiliza para agrupar los resultados que se incluyen en el hallazgo.

Si ha habilitado [la agregación entre regiones](#) y utiliza este cmdlet desde la región de agregación, el hallazgo se aplica a los resultados de la agregación y las regiones vinculadas.

Ejemplo

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "XXX"
    }
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = 'FAILED'
    }
}
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

Creación de un nuevo hallazgo personalizado a partir de un hallazgo administrado (solo para la consola)

No puede guardar los cambios en un hallazgo administrado ni eliminarlo. Sin embargo, puede utilizar hallazgos administrados como base para un nuevo hallazgo personalizado. Esta opción solo está disponible en la consola CSPM de Security Hub.

Para crear un nuevo hallazgo personalizado a partir de un hallazgo administrado (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Insights.
3. Elija el conocimiento administrado desde el que trabajar.
4. Edite la configuración de los hallazgos si es necesario.
 - Para cambiar el atributo utilizado para agrupar los resultados en el hallazgo:
 - a. Para eliminar la agrupación existente, elija la X situada junto al ajuste Agrupar por.

- b. Seleccione la barra de búsqueda.
- c. Seleccione el atributo que desea utilizar para el agrupamiento.
- d. Seleccione Aplicar.
- Para eliminar un filtro del hallazgo, elija la X rodeada de un círculo junto al filtro.
- Cómo agregar un filtro al hallazgo:
 - a. Seleccione la barra de búsqueda.
 - b. Seleccione el atributo y el valor que desea utilizar como filtro.
 - c. Seleccione Aplicar.
- 5. Cuando se hayan completado las actualizaciones, elija Create insight (Crear conocimiento).
- 6. Cuando se le solicite, escriba el Nombre del hallazgo; a continuación, elija Crear hallazgo.

Edición de hallazgos personalizados

Puede editar un hallazgo personalizado existente para cambiar el valor de agrupación y los filtros. Después de realizar los cambios, puede guardar las actualizaciones en el conocimiento original o guardar la versión actualizada como un nuevo conocimiento.

En AWS Security Hub Cloud Security Posture Management (CSPM), se puede utilizar información personalizada para recopilar un conjunto específico de hallazgos y realizar un seguimiento de los problemas que son exclusivos de su entorno. Para obtener información general sobre hallazgos personalizados, consulte [Descripción de la información personalizada en Security Hub \(CSPM\)](#).

Para editar un hallazgo personalizado, elija el método que prefiera y siga las instrucciones.

Security Hub CSPM console

Para editar un hallazgo personalizado (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Insights.
3. Elija el conocimiento personalizado que desea modificar.
4. Edite la configuración de los hallazgos si es necesario.
 - Para cambiar el atributo utilizado para agrupar los resultados en el hallazgo:
 - a. Para eliminar la agrupación existente, elija la X situada junto al ajuste Agrupar por.

- b. Seleccione la barra de búsqueda.
 - c. Seleccione el atributo que desea utilizar para el agrupamiento.
 - d. Seleccione Aplicar.
- Para eliminar un filtro del hallazgo, elija la X rodeada de un círculo junto al filtro.
- Cómo agregar un filtro al hallazgo:
 - a. Seleccione la barra de búsqueda.
 - b. Seleccione el atributo y el valor que desea utilizar como filtro.
 - c. Seleccione Aplicar.
- 5. Cuando complete las actualizaciones, elija Save insight (Guardar conocimiento).
- 6. Cuando se le solicite, siga uno de estos procedimientos:
 - Para actualizar la información existente para que refleje los cambios, seleccione Actualizar **<Insight_Name>** y, a continuación, seleccione Guardar información.
 - Para crear un nuevo conocimiento con las actualizaciones, elija Save new insight (Guardar nuevo conocimiento). Escriba un Insight name (Nombre del conocimiento) y elija Save insight (Guardar conocimiento).

Security Hub CSPM API

Para editar un hallazgo personalizado (API)

1. Utilice el [UpdateInsight](#) funcionamiento de la API CSPM de Security Hub. Si usa el comando, AWS CLI ejecute el [update-insight](#) comando.
2. Para identificar el hallazgo personalizado que desea actualizar, debe indicar su nombre de recurso de Amazon (ARN). Para obtener el ARN de un hallazgo personalizado, ejecute la operación [GetInsights](#) o el comando [get-insights](#).
3. Actualice los parámetros Name, Filters y GroupByAttribute según sea necesario.

En el siguiente ejemplo, se actualizan los hallazgos especificados. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE1111" --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value":
```

```
"AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --  
name "High severity role findings"
```

PowerShell

Para editar una información personalizada (PowerShell)

1. Utilice el cmdlet Update-SHUBInsight.
2. Para identificar el hallazgo personalizado, debe indicar su nombre de recurso de Amazon (ARN). Para obtener el ARN de un hallazgo personalizado, utilice el cmdlet Get-SHUBInsight.
3. Actualice los parámetros Name, Filter y GroupByAttribute según sea necesario.

Ejemplo

```
$Filter = @{  
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{  
        Comparison = "EQUALS"  
        Value = "AwsIamRole"  
    }  
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]@{  
        Comparison = "EQUALS"  
        Value = "HIGH"  
    }  
}  
  
Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-  
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-  
EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

Eliminación de hallazgos personalizados

En AWS Security Hub Cloud Security Posture Management (CSPM), se puede utilizar información personalizada para recopilar un conjunto específico de hallazgos y realizar un seguimiento de los problemas que son exclusivos de su entorno. Para obtener información general sobre hallazgos personalizados, consulte [Descripción de la información personalizada en Security Hub \(CSPM\)](#).

Para eliminar un hallazgo personalizado, elija el método que prefiera y siga las instrucciones. No puede eliminar un hallazgo administrado.

Security Hub CSPM console

Para eliminar un hallazgo personalizado (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Insights.
3. Localice el conocimiento personalizado que desea eliminar.
4. Para obtener ese hallazgo, elija el icono de más opciones (los tres puntos en la esquina superior derecha de la tarjeta).
5. Elija Eliminar.

Security Hub CSPM API

Para eliminar un hallazgo personalizado (API)

1. Utilice el [DeleteInsight](#) funcionamiento de la API CSPM de Security Hub. Si usa el comando, AWS CLI ejecute el [delete-insight](#) comando.
2. Para identificar el hallazgo personalizado que se va a eliminar, indique su ARN. Para obtener el ARN de un hallazgo personalizado, ejecute la operación [GetInsights](#) o el comando [get-insights](#).

En el siguiente ejemplo, se elimina el hallazgo especificado. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

PowerShell

Para eliminar una información personalizada (PowerShell)

1. Utilice el cmdlet `Remove-SHUBInsight`.
2. Para identificar el hallazgo personalizado, indique su ARN. Para obtener el ARN de un hallazgo personalizado, utilice el cmdlet `Get-SHUBInsight`.

Ejemplo

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Modificación automática de los hallazgos en Security Hub (CSPM) y acción en función de ellos

AWS Security Hub Cloud Security Posture Management (CSPM) tiene funciones que modifican automáticamente los hallazgos y toman medidas en función de sus especificaciones.

Security Hub CSPM admite actualmente dos tipos de automatizaciones:

- **Reglas de automatización:** Actualice y suprima automáticamente los resultados casi en tiempo real en función de los criterios que defina.
- **Respuesta y corrección automatizadas:** cree EventBridge reglas de Amazon personalizadas que definan las acciones automáticas que se deben tomar en función de hallazgos e información específicos.

Las reglas de automatización son útiles cuando se desean actualizar automáticamente los campos de búsqueda en el formato de búsqueda AWS de seguridad (ASFF). Por ejemplo, puede utilizar una regla de automatización para actualizar el nivel de gravedad o el estado del flujo de trabajo de los resultados de una integración específica de terceros. El uso de la regla de automatización elimina la necesidad de actualizar de manera manual el nivel de gravedad o el estado del flujo de trabajo de cada resultado de este producto de terceros.

EventBridge las reglas son útiles cuando quieres tomar medidas fuera del Security Hub CSPM con respecto a hallazgos específicos o enviar hallazgos específicos a herramientas de terceros para su corrección o investigación adicional. Las reglas se pueden utilizar para activar acciones compatibles, como invocar una AWS Lambda función o notificar a un tema del Amazon Simple Notification Service (Amazon SNS) sobre un hallazgo específico.

Las reglas de automatización entran en vigor antes de que se EventBridge apliquen. Es decir, las reglas de automatización se activan y actualizan un hallazgo EventBridge antes de recibirlo. EventBridge Las reglas se aplican entonces al hallazgo actualizado.

Al configurar automatizaciones para los controles de seguridad, recomendamos filtrar en función del ID del control en vez del título o la descripción. Mientras que Security Hub CSPM actualiza ocasionalmente los títulos y descripciones de los controles, el control sigue IDs siendo el mismo.

Temas

- [Descripción de las reglas de automatización en Security Hub CSPM](#)

- [Uso EventBridge para respuesta y remediación automatizadas](#)

Descripción de las reglas de automatización en Security Hub CSPM

Puede utilizar las reglas de automatización para actualizar automáticamente los resultados en AWS Security Hub Cloud Security Posture Management (CSPM). A medida que incorpora los hallazgos, Security Hub CSPM puede aplicar una variedad de acciones de reglas, como suprimir los hallazgos, cambiar su gravedad y agregar notas. Estas acciones de reglas modifican los resultados que coinciden con criterios específicos.

Algunos ejemplos de casos de uso de reglas de automatización son los siguientes:

- Elevar la gravedad de un resultado a CRITICAL si el ID de recurso del resultado se refiere a un recurso crítico para la empresa.
- Elevar la gravedad de un resultado de HIGH a CRITICAL si el resultado afecta a recursos en cuentas de producción específicas.
- Asignar resultados específicos que tengan una gravedad INFORMATIONAL un estado de flujo de trabajo SUPPRESSED.

Puede crear y gestionar reglas de automatización únicamente desde una cuenta de administrador CSPM de Security Hub.

Las reglas se aplican a los resultados tanto nuevos como actualizados. Puede crear una regla personalizada desde cero o utilizar una plantilla de regla proporcionada por Security Hub CSPM. Además, puede empezar con una plantilla y modificarla según sea necesario.

Definición de criterios de regla y acciones de regla

Desde una cuenta de administrador de CSPM de Security Hub, puede crear una regla de automatización definiendo uno o más criterios de regla y una o más acciones de regla. Cuando un hallazgo coincide con los criterios definidos, Security Hub CSPM le aplica las acciones de la regla. Para obtener más información sobre los criterios y acciones disponibles, consulte [Criterios de regla y acciones de regla disponibles](#).

Security Hub CSPM admite actualmente un máximo de 100 reglas de automatización para cada cuenta de administrador.

La cuenta de administrador CSPM de Security Hub también puede editar, ver y eliminar reglas de automatización. Una regla se aplica a los resultados que coinciden en la cuenta de administrador y en todas las cuentas de miembro. Al proporcionar la cuenta de miembro IDs como criterio de regla, los administradores de CSPM de Security Hub también pueden usar reglas de automatización para actualizar o suprimir los hallazgos en cuentas de miembros específicas.

Una regla de automatización solo se aplica en el lugar Región de AWS en el que se creó. Para aplicar una regla en varias regiones, el administrador debe crear la regla en cada región. Esto se puede hacer a través de la consola CSPM de Security Hub, la API CSPM de Security Hub o. [AWS CloudFormation](#) [También puede utilizar un script de despliegue multirregional.](#)

Criterios de regla y acciones de regla disponibles

Los siguientes campos del formato de búsqueda de AWS seguridad (ASFF) se admiten actualmente como criterios para las reglas de automatización:

Criterio de regla	Operadores de filtro	Tipo de campo
AwsAccountId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
AwsAccountName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
CompanyName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
ComplianceAssociatedStandardsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena

Criterio de regla	Operadores de filtro	Tipo de campo
ComplianceSecurityControlId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
ComplianceStatus	Is, Is Not	Selección: [FAILED, NOT_AVAILABLE, PASSED, WARNING]
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Número
CreatedAt	Start, End, DateRange	Fecha (formateada como 2022-12-01T21:47:39.269Z)
Criticality	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Número
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
FirstObservedAt	Start, End, DateRange	Fecha (formateada como 2022-12-01T21:47:39.269Z)
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena

Criterio de regla	Operadores de filtro	Tipo de campo
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
LastObservedAt	Start, End, DateRange	Fecha (formateada como 2022-12-01T21:47:39.269Z)
NoteText	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
NoteUpdatedAt	Start, End, DateRange	Fecha (formateada como 2022-12-01T21:47:39.269Z)
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena

Criterio de regla	Operadores de filtro	Tipo de campo
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Asignación
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena

Criterio de regla	Operadores de filtro	Tipo de campo
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Asignación
ResourceType	Is, Is Not	Selección (consulte los recursos admitidos por ASFF)
SeverityLabel	Is, Is Not	Selección: [CRITICAL, HIGH, MEDIUM, LOW, INFORMATIONAL]
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
UpdatedAt	Start, End, DateRange	Fecha (formateada como 2022-12-01T21:47:39.269Z)

Criterio de regla	Operadores de filtro	Tipo de campo
UserDefinedFields	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Asignación
VerificationState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Cadena
WorkflowStatus	Is, Is Not	Selección: [NEW, NOTIFIED, RESOLVED, SUPPRESSED]

En el caso de los criterios etiquetados como campos de cadena, el uso de diferentes operadores de filtro en un mismo campo afecta a la lógica de evaluación. Para obtener más información, consulte la referencia [StringFilter](#) de la API AWS de administración de posturas de seguridad (CSPM) de Security Hub Cloud.

Cada criterio admite una cantidad máxima de valores que se pueden utilizar para filtrar los resultados que coinciden. Para conocer los límites de cada criterio, consulte la referencia de [AutomationRulesFindingFilters](#) la API AWS de gestión de la postura de seguridad (CSPM) de Security Hub Cloud.

Actualmente se admiten los siguientes campos ASFF como acciones para las reglas de automatización:

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

Para obtener más información sobre campos ASFF específicos, consulte la sintaxis del [formato de búsqueda AWS de seguridad \(ASFF\)](#).

 Tip

Si desea que Security Hub CSPM deje de generar hallazgos para un control específico, le recomendamos que desactive el control en lugar de utilizar una regla de automatización. Cuando deshabilita un control, Security Hub CSPM deja de ejecutar controles de seguridad en él y deja de generar resultados para él, por lo que no incurrirá en cargos por ese control. Le recomendamos que utilice reglas de automatización para cambiar los valores de campos ASFF específicos para los resultados que coincidan con los criterios definidos. Para obtener más información sobre cómo deshabilitar controles, consulte [Desactivación de los controles en Security Hub \(CSPM\)](#).

Resultados que las reglas de automatización evalúan

Una regla de automatización evalúa los hallazgos nuevos y actualizados que Security Hub CSPM genera o ingiere a través de la [BatchImportFindings](#) operación después de crear la regla. Security Hub CSPM actualiza las conclusiones de control cada 12-24 horas o cuando el recurso asociado cambia de estado. Para obtener más información, consulte [Programación para ejecución de controles de seguridad](#).

Las reglas de automatización evalúan los resultados originales proporcionados por el proveedor. Los proveedores pueden proporcionar nuevos hallazgos y actualizar los hallazgos existentes mediante el BatchImportFindings funcionamiento de la API CSPM de Security Hub. Las reglas no se desencadenan cuando se actualizan los campos de resultados después de la creación de la regla mediante la operación [BatchUpdateFindings](#). Si crea una regla de automatización y realiza una actualización BatchUpdateFindings que afecten al mismo campo de resultado, la última actualización establecerá el valor de ese campo. Vea el siguiente ejemplo:

1. Se utiliza BatchUpdateFindings para actualizar el campo Workflow.Status de un resultado de NEW a NOTIFIED.
2. Si llama a GetFindings, el campo Workflow.Status ahora tendrá un valor de NOTIFIED.
3. Se crea una regla de automatización que cambia el campo Workflow.Status del resultado de NEW a SUPPRESSED (recuerde que las reglas ignoran las actualizaciones realizadas con BatchUpdateFindings).

4. El proveedor de resultados utiliza `BatchImportFindings` para actualizar el resultado y cambia el campo `Workflow.Status` a `NEW`.
5. Si llama a `GetFindings`, el campo `Workflow.Status` ahora tendrá un valor de `SUPPRESSED`, ya que se aplicará la regla de automatización y la regla será la última acción que se realice en el resultado.

Al crear o editar una regla en la consola CSPM de Security Hub, la consola muestra una versión beta de los resultados que coinciden con los criterios de la regla. Mientras que las reglas de automatización evalúan las conclusiones originales enviadas por el proveedor de la búsqueda, la versión beta de la consola refleja las conclusiones en su estado final, tal como se mostrarían en respuesta a la operación de la [GetFindings](#) API (es decir, después de aplicar las acciones de la regla u otras actualizaciones a la conclusión).

Cómo funciona el orden de las reglas

Al crear reglas de automatización, usted asigna a cada regla un orden. Esto determina el orden en el que Security Hub CSPM aplica las reglas de automatización y adquiere importancia cuando varias reglas se relacionan con el mismo campo de búsqueda o búsqueda.

Cuando varias acciones de reglas se refieren al mismo resultado o campo de resultado, la regla con el valor numérico más alto de orden de reglas se aplica en último lugar y tiene el efecto definitivo.

Al crear una regla en la consola CSPM de Security Hub, Security Hub CSPM asigna automáticamente el orden de las reglas en función del orden de creación de la regla. La regla creada más recientemente tiene el valor numérico más bajo de orden de reglas y, por lo tanto, se aplica primero. Security Hub CSPM aplica las reglas subsiguientes en orden ascendente.

Al crear una regla a través de la API CSPM de Security Hub o AWS CLI, Security Hub CSPM aplica primero la regla con el valor numérico más bajo. `RuleOrder` Luego aplica las reglas subsiguientes en orden ascendente. Si varios resultados tienen lo mismo `RuleOrder`, Security Hub CSPM aplica primero una regla con un valor anterior para el `UpdatedAt` campo (es decir, la regla que se editó más recientemente se aplica en último lugar).

Puede modificar el orden de las reglas en cualquier momento.

Ejemplo de orden de reglas:

Regla A (el orden de la regla es **1**):

- Criterios de la regla A
 - `ProductName = Security Hub CSPM`
 - `Resources.Type` es S3 Bucket
 - `Compliance.Status = FAILED`
 - `RecordState` es NEW
 - `Workflow.Status = ACTIVE`
- Acciones de la regla A
 - Actualizar Confidence a 95
 - Actualizar Severity a CRITICAL

Regla B (el orden de la regla es2):

- Criterios de la regla B
 - `AwsAccountId = 123456789012`
- Acciones de la regla B
 - Actualizar Severity a INFORMATIONAL

Las acciones de la regla A se aplican primero a las conclusiones del CSPM de Security Hub que coinciden con los criterios de la regla A. A continuación, las acciones de la Regla B se aplican a los hallazgos de CSPM de Security Hub con el ID de cuenta especificado. En este ejemplo, como la regla B se aplica en último lugar, el valor final de Severity en los resultados del ID de cuenta especificado es INFORMATIONAL. Según la acción de la regla A, el valor final de Confidence en los resultados coincidentes es 95.

Creación de reglas de automatización

Se puede usar una regla de automatización para actualizar automáticamente los hallazgos en AWS Security Hub Cloud Security Posture Management (CSPM). Puede crear una regla de automatización personalizada desde cero o, en la consola CSPM de Security Hub, utilizar una plantilla de reglas rellena previamente. Para obtener información general sobre cómo funcionan las reglas de automatización, consulte [Descripción de las reglas de automatización en Security Hub CSPM](#).

Solo puede crear una regla de automatización a la vez. Para crear varias reglas de automatización, siga los procedimientos de la consola tantas veces como necesite o llame a la API o al comando tantas veces como necesite con los parámetros que desee.

Debe crear una regla de automatización en cada región y cuenta en que desee que la regla se aplique a los resultados.

Al crear una regla de automatización en la consola CSPM de Security Hub, Security Hub CSPM le muestra una versión beta de los resultados a los que se aplica la regla. La versión beta no es compatible actualmente si los criterios de la regla incluyen un filtro CONTAINS o NOT_CONTAINS. Puede elegir estos filtros para los tipos de campos de mapeo y cadena.

 Important

AWS recomienda no incluir información de identificación personal, confidencial o delicada en el nombre, la descripción u otros campos de la regla.

Creación de una regla de automatización personalizada

Elija su método preferido y realice los siguientes pasos para crear una regla de automatización personalizada.

Console

Para crear una regla de automatización personalizada (consola)

1. Con las credenciales del administrador CSPM de Security Hub, abra la consola de AWS Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, seleccione Automatizaciones.
3. Seleccione Crear regla. En Tipo de regla, seleccione Crear regla personalizada.
4. En la sección Regla, proporcione un nombre de regla único y una descripción de la regla.
5. En Criterios, utilice los menús desplegables de Clave, Operador y Valor para especificar los criterios de su regla. Debe especificar al menos un criterio de regla.

Si es compatible con los criterios seleccionados, la consola le mostrará una versión beta de los resultados que coincidan con sus criterios.

6. En Acción automatizada, utilice los menús desplegables para especificar qué campos de resultado desea actualizar cuando los resultados coincidan con los criterios de la regla. Debe especificar al menos una regla de acción.

7. En Estado de la regla, elija si desea que la regla quede Habilitada o Deshabilitada tras su creación.
8. (Opcional) Amplíe la sección Ajustes adicionales. Seleccione Ignorar reglas posteriores para resultados que coincidan con estos criterios si desea que esta regla sea la última que se aplique a los resultados que coincidan con los criterios de la regla.
9. (Opcional) En Etiquetas, añada etiquetas como pares clave-valor para ayudarle a identificar fácilmente la regla.
10. Seleccione Creación de regla.

API

Para crear una regla de automatización personalizada (API)

1. Ejecute [CreateAutomationRule](#) desde la cuenta de administrador CSPM de Security Hub. Esta API crea una regla con un nombre de recurso de Amazon (ARN) específico.
2. Introduzca un nombre y una descripción para la regla.
3. Defina el parámetro `IsTerminal` como `true` si desea que esta regla sea la última que se aplique a los resultados que coincidan con los criterios de la regla.
4. En el parámetro `RuleOrder`, indique el orden de la regla. Security Hub CSPM aplica primero las reglas con un valor numérico inferior para este parámetro.
5. Para el `RuleStatus` parámetro, especifique si desea que Security Hub CSPM habilite y comience a aplicar la regla a las conclusiones tras su creación. El valor predeterminado es `ENABLED` si no se especifica ningún valor. Un valor de `DISABLED` significa que la regla queda en pausa tras su creación.
6. Para el `Criteria` parámetro, indique los criterios que desea que utilice Security Hub CSPM para filtrar sus hallazgos. La acción de la regla se aplicará a los resultados que coincidan con los criterios. Para obtener una lista de los criterios admitidos, consulte [Criterios de regla y acciones de regla disponibles](#).
7. Para el `Actions` parámetro, indique las acciones que desee que realice Security Hub CSPM cuando haya una coincidencia entre un hallazgo y los criterios definidos. Para obtener una lista de las acciones admitidas, consulte [Criterios de regla y acciones de regla disponibles](#).

El siguiente AWS CLI comando de ejemplo crea una regla de automatización que actualiza el estado del flujo de trabajo y anota los resultados coincidentes. Este ejemplo está formateado

para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub create-automation-rule \
--actions '[{
  "Type": "FINDING_FIELDS_UPDATE",
  "FindingFieldsUpdate": {
    "Severity": {
      "Label": "HIGH"
    },
    "Note": {
      "Text": "Known issue that is a risk. Updated by automation rules",
      "UpdatedBy": "sechub-automation"
    }
  }
}]' \
--criteria '{
  "SeverityLabel": [{
    "Value": "INFORMATIONAL",
    "Comparison": "EQUALS"
  }]
}' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
--region us-east-1
```

Crear una regla de automatización a partir de una plantilla (solo en la consola)

Las plantillas de reglas reflejan casos de uso comunes para las reglas de automatización. Actualmente, solo la consola CSPM de Security Hub admite plantillas de reglas. Complete los siguientes pasos para crear una regla de automatización a partir de una plantilla en la consola.

Para crear una regla de automatización a partir de una plantilla (en la consola)

1. Con las credenciales del administrador CSPM de Security Hub, abra la consola de AWS Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, seleccione Automatizaciones.

3. Seleccione Crear regla. En Tipo de regla, elija Crear una regla a partir de una plantilla.
4. Seleccione una plantilla de regla en el menú desplegable.
5. (Opcional) De ser necesario para su caso de uso, modifique las secciones Regla, Criterios y Acción automatizada. Debe especificar al menos un criterio de regla y una acción de regla.

Si es compatible con los criterios seleccionados, la consola le mostrará una versión beta de los resultados que coincidan con sus criterios.

6. En Estado de la regla, elija si desea que la regla quede Habilitada o Deshabilitada tras su creación.
7. (Opcional) Amplíe la sección Ajustes adicionales. Seleccione Ignorar reglas posteriores para resultados que coincidan con estos criterios si desea que esta regla sea la última que se aplique a los resultados que coincidan con los criterios de la regla.
8. (Opcional) En Etiquetas, añada etiquetas como pares clave-valor para ayudarle a identificar fácilmente la regla.
9. Seleccione Creación de regla.

Visualización de las reglas de automatización

Se puede usar una regla de automatización para actualizar automáticamente los hallazgos en AWS Security Hub Cloud Security Posture Management (CSPM). Para obtener información general sobre cómo funcionan las reglas de automatización, consulte [Descripción de las reglas de automatización en Security Hub CSPM](#).

Elija el método que prefiera y siga los pasos para ver sus reglas de automatización existentes y los detalles de cada regla.

Para obtener un historial de cómo las reglas de automatización han modificado sus resultados, consulte [Revisión de los detalles y el historial de búsquedas en Security Hub \(CSPM\)](#).

Console

Para ver las reglas de automatización (consola)

1. Con las credenciales del administrador CSPM de Security Hub, abra la consola de AWS Security Hub Cloud Security Posture Management (CSPM) en: <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, seleccione Automatizaciones.

3. Elija un nombre de regla. También puede seleccionar una regla.
4. Seleccione Acciones y luego Ver.

API

Para ver las reglas de automatización (API)

1. Para ver las reglas de automatización de su cuenta, ejecútelo [ListAutomationRules](#) desde la cuenta de administrador CSPM de Security Hub. Esta API devuelve la regla ARNs y otros metadatos de sus reglas. No se requieren parámetros de entrada para esta API, pero puede como opción proporcionar `MaxResults` para limitar el número de resultados y `NextToken` como parámetro de paginación. El valor inicial de `NextToken` debería ser `NULL`.
2. Para obtener información adicional sobre la regla, incluidos los criterios y las acciones de una regla, ejecútela [BatchGetAutomationRules](#) desde la cuenta de administrador CSPM de Security Hub. Proporcione las reglas ARNs de automatización de las que desee obtener detalles.

En el siguiente ejemplo, se recuperan los detalles de las reglas de automatización especificadas. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (`\`) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub batch-get-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-
east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
"arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222"]' \
--region us-east-1
```

Edición de reglas de automatización

Se puede usar una regla de automatización para actualizar automáticamente los hallazgos en AWS Security Hub Cloud Security Posture Management (CSPM). Para obtener información general sobre cómo funcionan las reglas de automatización, consulte [Descripción de las reglas de automatización en Security Hub CSPM](#).

Tras crear una regla de automatización, el administrador CSPM de Security Hub delegado puede editar la regla. Al editar una regla de automatización, los cambios se aplican a los hallazgos nuevos y actualizados que Security Hub CSPM genera o ingiere después de editar la regla.

Elija el método que prefiera y siga los pasos para editar el contenido de una regla de automatización. Puede editar una o más reglas con una sola solicitud. Para obtener instrucciones sobre cómo editar el orden de las reglas, consulte [Edición del orden de las reglas de automatización](#).

Console

Para editar las reglas de automatización (consola)

1. Con las credenciales del administrador CSPM de Security Hub, abra la consola de AWS Security Hub Cloud Security Posture Management (CSPM) en: <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, seleccione Automatizaciones.
3. Seleccione la regla que desea editar. Seleccione Acciones y luego Editar.
4. Cambie la regla como desee y seleccione Guardar cambios.

API

Para editar las reglas de automatización (API)

1. Ejecute [BatchUpdateAutomationRules](#) desde la cuenta de administrador CSPM de Security Hub.
2. En el parámetro RuleArn, proporcione el ARN de las reglas que desee editar.
3. Proporcione los nuevos valores de los parámetros que desee editar. Puede editar cualquier parámetro excepto RuleArn.

En el siguiente ejemplo, se actualiza la regla de automatización especificada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
{
  "Actions": [{
    "Type": "FINDING_FIELDS_UPDATE",
```



```

    "FindingFieldsUpdate": {
      "Note": {
        "Text": "Known issue that is a risk",
        "UpdatedBy": "sechub-automation"
      },
      "Workflow": {
        "Status": "NEW"
      }
    },
  ],
  "Criteria": {
    "SeverityLabel": [{
      "Value": "LOW",
      "Comparison": "EQUALS"
    }]
  },
  "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "RuleOrder": 14,
  "RuleStatus": "DISABLED",
}
]' \
--region us-east-1

```

Edición del orden de las reglas de automatización

Se puede usar una regla de automatización para actualizar automáticamente los hallazgos en AWS Security Hub Cloud Security Posture Management (CSPM). Para obtener información general sobre cómo funcionan las reglas de automatización, consulte [Descripción de las reglas de automatización en Security Hub CSPM](#).

Tras crear una regla de automatización, el administrador CSPM de Security Hub delegado puede editar la regla.

Si desea mantener los criterios y las acciones de la regla iguales, pero cambiar el orden en el que Security Hub CSPM aplica una regla de automatización, puede editar solo el orden de las reglas. Elija el método que prefiera y siga los pasos para editar el orden de las reglas.

Para obtener instrucciones acerca de cómo editar los criterios o las acciones de una regla de automatización, consulte [Edición de reglas de automatización](#).

Console

Para editar el orden de una regla de automatización (consola)

1. Con las credenciales del administrador CSPM de Security Hub, abra la consola de AWS Security Hub Cloud Security Posture Management (CSPM) en: <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, seleccione Automatizaciones.
3. Seleccione la regla cuyo orden desea modificar. Seleccione Editar prioridad.
4. Seleccione Subir para aumentar la prioridad de la regla en una unidad. Seleccione Bajar para disminuir la prioridad de la regla en una unidad. Seleccione Mover al principio para asignar a la regla un orden de 1 (esto da a la regla precedencia sobre otras existentes).

Note

Al crear una regla en la consola CSPM de Security Hub, Security Hub CSPM asigna automáticamente el orden de las reglas en función del orden de creación de la regla. La regla creada más recientemente tiene el valor numérico más bajo de orden de reglas y, por lo tanto, se aplica primero.

API

Para editar el orden de una regla de automatización (API)

1. Utilice la [BatchUpdateAutomationRules](#) operación desde la cuenta de administrador CSPM de Security Hub.
2. En el parámetro RuleArn, proporcione el ARN de las reglas cuyo orden desea editar.
3. Modifique el valor del campo RuleOrder.

Note

Si varias reglas tienen lo mismo RuleOrder, Security Hub CSPM aplica primero una regla con un valor anterior para el UpdatedAt campo (es decir, la regla que se editó más recientemente se aplica en último lugar).

Eliminación o desactivación de las reglas de automatización

Se puede usar una regla de automatización para actualizar automáticamente los hallazgos en AWS Security Hub Cloud Security Posture Management (CSPM). Para obtener información general sobre cómo funcionan las reglas de automatización, consulte [Descripción de las reglas de automatización en Security Hub CSPM](#).

Cuando eliminas una regla de automatización, Security Hub CSPM la elimina de tu cuenta y deja de aplicarla a los hallazgos. Como alternativa a la eliminación, puede desactivar una regla. Esto conserva la regla para usarla en el futuro, pero Security Hub CSPM no aplicará la regla a ningún hallazgo coincidente hasta que la habilites.

Elija el método que prefiera y siga los pasos para eliminar una regla de automatización. Puede eliminar una o más reglas en una sola solicitud.

Console

Para eliminar o desactivar las reglas de automatización (consola)

1. Con las credenciales del administrador CSPM de Security Hub, abra la consola de AWS Security Hub Cloud Security Posture Management (CSPM) en: <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, seleccione Automatizaciones.
3. Seleccione las reglas que desea eliminar. Seleccione Acción y luego Eliminar (para retener una regla, pero temporalmente deshabilitada, seleccione Deshabilitar).
4. Confirme la elección y seleccione Eliminar.

API

Para eliminar o desactivar las reglas de automatización (API)

1. Utilice la [BatchDeleteAutomationRules](#) operación desde la cuenta de administrador CSPM de Security Hub.
2. En el parámetro AutomationRulesArns, indique el ARN de las reglas que desea eliminar (para retener una regla, pero temporalmente deshabilitada, indique DISABLED en el parámetro RuleStatus).

En el siguiente ejemplo, se elimina la regla de automatización que se especificó. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE1111"]' \
--region us-east-1
```

Ejemplos de reglas de automatización

En esta sección se proporcionan ejemplos de reglas de automatización para casos de uso comunes de CSPM de Security Hub. Estos ejemplos corresponden a plantillas de reglas que están disponibles en la consola CSPM de Security Hub.

Elevar la gravedad a Crítica cuando un recurso específico como un bucket S3 esté en riesgo

En este ejemplo, los criterios de la regla coinciden cuando el ResourceId de un resultado es un bucket específico de Amazon Simple Storage Service (Amazon S3). La acción de la regla es cambiar la gravedad de los resultados coincidentes a CRITICAL. Puede modificar esta plantilla para aplicarla a otros recursos.

Ejemplo de solicitud de API:

```
{
  "IsTerminal": true,
  "RuleName": "Elevate severity of findings that relate to important resources",
  "RuleOrder": 1,
  "RuleStatus": "ENABLED",
  "Description": "Elevate finding severity to CRITICAL when specific resource such as
an S3 bucket is at risk",
  "Criteria": {
    "ProductName": [{
      "Value": "Security Hub CSPM",
      "Comparison": "EQUALS"
    }],
    "ComplianceStatus": [{
      "Value": "FAILED",
      "Comparison": "EQUALS"
    }]
  }
}
```

```

    }],
    "RecordState": [{
      "Value": "ACTIVE",
      "Comparison": "EQUALS"
    }],
    "WorkflowStatus": [{
      "Value": "NEW",
      "Comparison": "EQUALS"
    }],
    "ResourceId": [{
      "Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
      "Comparison": "EQUALS"
    }]
  },
  "Actions": [{
    "Type": "FINDING_FIELDS_UPDATE",
    "FindingFieldsUpdate": {
      "Severity": {
        "Label": "CRITICAL"
      },
      "Note": {
        "Text": "This is a critical resource. Please review ASAP.",
        "UpdatedBy": "sechub-automation"
      }
    }
  ]
}]
}

```

Ejemplo de comando de la CLI:

```

$
aws securityhub create-automation-rule \
--is-terminal \
--rule-name "Elevate severity of findings that relate to important resources" \
--rule-order 1 \
--rule-status "ENABLED" \

--description "Elevate finding severity to CRITICAL when specific resource such as an
S3 bucket is at risk" \
--criteria '{
"ProductName": [{
"Value": "Security Hub CSPM",
"Comparison": "EQUALS"

```

```

    }],
    "ComplianceStatus": [{
      "Value": "FAILED",
      "Comparison": "EQUALS"
    }],
    "RecordState": [{
      "Value": "ACTIVE",
      "Comparison": "EQUALS"
    }],
    "WorkflowStatus": [{
      "Value": "NEW",
      "Comparison": "EQUALS"
    }],
    "ResourceId": [{
      "Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
      "Comparison": "EQUALS"
    }]
  }' \
  --actions '[{
    "Type": "FINDING_FIELDS_UPDATE",
    "FindingFieldsUpdate": {
      "Severity": {
        "Label": "CRITICAL"
      },
      "Note": {
        "Text": "This is a critical resource. Please review ASAP.",
        "UpdatedBy": "sechub-automation"
      }
    }
  }]' \
  --region us-east-1

```

Cómo elevar la gravedad de los resultados relacionados con los recursos en cuentas de producción

En este ejemplo, los criterios de la regla coinciden cuando se genera un resultado de gravedad HIGH en cuentas de producción específicas. La acción de la regla es cambiar la gravedad de los resultados coincidentes a CRITICAL.

Ejemplo de solicitud de API:

```

{
  "IsTerminal": false,

```

```

"RuleName": "Elevate severity for production accounts",
"RuleOrder": 1,
"RuleStatus": "ENABLED",
"Description": "Elevate finding severity from HIGH to CRITICAL for findings that
relate to resources in specific production accounts",
"Criteria": {
  "ProductName": [{
    "Value": "Security Hub CSPM",
    "Comparison": "EQUALS"
  }],
  "ComplianceStatus": [{
    "Value": "FAILED",
    "Comparison": "EQUALS"
  }],
  "RecordState": [{
    "Value": "ACTIVE",
    "Comparison": "EQUALS"
  }],
  "WorkflowStatus": [{
    "Value": "NEW",
    "Comparison": "EQUALS"
  }],
  "SeverityLabel": [{
    "Value": "HIGH",
    "Comparison": "EQUALS"
  }],
  "AwsAccountId": [
    {
      "Value": "111122223333",
      "Comparison": "EQUALS"
    },
    {
      "Value": "123456789012",
      "Comparison": "EQUALS"
    }
  ]
},
"Actions": [{
  "Type": "FINDING_FIELDS_UPDATE",
  "FindingFieldsUpdate": {
    "Severity": {
      "Label": "CRITICAL"
    },
    "Note": {

```

```

        "Text": "A resource in production accounts is at risk. Please review
        ASAP.",
        "UpdatedBy": "sechub-automation"
    }
}
}]
}

```

Ejemplo de comando de la CLI:

```

aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Elevate severity of findings that relate to resources in production
accounts" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate
to resources in specific production accounts" \
--criteria '{
"ProductName": [{
"Value": "Security Hub CSPM",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "HIGH",
"Comparison": "EQUALS"
}],
"AwsAccountId": [
{
"Value": "111122223333",
"Comparison": "EQUALS"
},
{
"Value": "123456789012",

```



```

"Comparison": "EQUALS"
}]
}' \
--actions '[{
  "Type": "FINDING_FIELDS_UPDATE",
  "FindingFieldsUpdate": {
    "Severity": {
      "Label": "CRITICAL"
    },
    "Note": {
      "Text": "A resource in production accounts is at risk. Please review ASAP.",
      "UpdatedBy": "sechub-automation"
    }
  }
}]' \
--region us-east-1

```

Cómo suprimir resultados informativos

En este ejemplo, los criterios de la regla coinciden con los hallazgos de INFORMATIONAL gravedad enviados a Security Hub CSPM desde Amazon. GuardDuty La acción de la regla es cambiar el estado del flujo de trabajo de los resultados coincidentes a SUPPRESSED.

Ejemplo de solicitud de API:

```

{
  "IsTerminal": false,
  "RuleName": "Suppress informational findings",
  "RuleOrder": 1,
  "RuleStatus": "ENABLED",
  "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
  "Criteria": {
    "ProductName": [{
      "Value": "GuardDuty",
      "Comparison": "EQUALS"
    }],
    "RecordState": [{
      "Value": "ACTIVE",
      "Comparison": "EQUALS"
    }],
    "WorkflowStatus": [{
      "Value": "NEW",
      "Comparison": "EQUALS"
    }],
  }
}

```

```

    }],
    "SeverityLabel": [{
      "Value": "INFORMATIONAL",
      "Comparison": "EQUALS"
    }]
  },
  "Actions": [{
    "Type": "FINDING_FIELDS_UPDATE",
    "FindingFieldsUpdate": {
      "Workflow": {
        "Status": "SUPPRESSED"
      },
      "Note": {
        "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",
        "UpdatedBy": "sechub-automation"
      }
    }
  }]
}

```

Ejemplo de comando de la CLI:

```

aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
--criteria '{
"ProductName": [{
"Value": "GuardDuty",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}]
}'

```

```

"WorkflowStatus": [{
  "Value": "NEW",
  "Comparison": "EQUALS"
}],
"SeverityLabel": [{
  "Value": "INFORMATIONAL",
  "Comparison": "EQUALS"
}]
}' \
--actions '[{
  "Type": "FINDING_FIELDS_UPDATE",
  "FindingFieldsUpdate": {
    "Workflow": {
      "Status": "SUPPRESSED"
    },
    "Note": {
      "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",
      "UpdatedBy": "sechub-automation"
    }
  }
}]' \
--region us-east-1

```

Uso EventBridge para respuesta y remediación automatizadas

Al crear reglas en Amazon EventBridge, puedes responder automáticamente a las conclusiones de AWS Security Hub Cloud Security Posture Management (CSPM). Security Hub CSPM envía los resultados en forma de eventos casi EventBridge en tiempo real. Puede crear reglas sencillas para indicar qué eventos le resultan de interés, así como qué acciones automatizadas se van a realizar cuando un evento cumple una de las reglas. Entre las acciones que se pueden activar automáticamente se incluyen las siguientes:

- Invocar una función AWS Lambda
- Invocar el comando Amazon EC2 run
- Desviar el evento a Amazon Kinesis Data Streams
- Activar una máquina de AWS Step Functions estados
- Notificar un tema de Amazon SNS o una cola de Amazon SQS
- Enviar un resultado a una herramienta de gestión de tickets, chat, de SIEM o respuesta a incidentes de terceros

Security Hub CSPM envía automáticamente todos los hallazgos nuevos y todas las actualizaciones de los hallazgos existentes a EventBridge as EventBridge events. También puede crear acciones personalizadas que le permitan enviar los hallazgos seleccionados y los resultados de información a EventBridge

A continuación, configura EventBridge las reglas para responder a cada tipo de evento.

Para obtener más información sobre el uso EventBridge, consulta la [Guía del EventBridge usuario de Amazon](#).

Note

Como práctica recomendada, asegúrate de que los permisos de acceso concedidos a tus usuarios EventBridge utilicen políticas de privilegios mínimos AWS Identity and Access Management (IAM) que concedan únicamente los permisos necesarios.

Para obtener más información, consulta [Gestión de identidad y acceso en Amazon EventBridge](#).

En Soluciones también hay disponible un conjunto de plantillas para la respuesta y la corrección automatizadas entre cuentas. AWS Las plantillas aprovechan las reglas de EventBridge eventos y las funciones Lambda. La solución se implementa mediante AWS CloudFormation y. AWS Systems Manager La solución puede crear acciones de respuesta y corrección totalmente automatizadas. También puede usar las acciones personalizadas CSPM de Security Hub para crear acciones de respuesta y remediación activadas por el usuario. Para obtener más información sobre cómo configurar y utilizar la solución, consulte la página de la solución [Respuesta de seguridad automatizada en AWS](#).

Temas

- [Tipos de eventos CSPM de Security Hub en EventBridge](#)
- [EventBridge formatos de eventos para Security Hub CSPM](#)
- [Configuración de una EventBridge regla para las conclusiones del CSPM de Security Hub](#)
- [Utilizar acciones personalizadas para enviar las conclusiones y los resultados de información a EventBridge](#)

Tipos de eventos CSPM de Security Hub en EventBridge

Security Hub CSPM utiliza los siguientes tipos de EventBridge eventos de Amazon para integrarse. EventBridge

En el EventBridge panel de control de Security Hub CSPM, All Events incluye todos estos tipos de eventos.

Todos los resultados (Security Hub Findings - Imported)

Security Hub CSPM envía automáticamente todos los hallazgos nuevos y todas las actualizaciones de los hallazgos existentes a EventBridge as Security Hub Findings - Imported events. Cada evento Security Hub Findings - Imported contiene un único resultado.

Cada solicitud [BatchImportFindings](#) y [BatchUpdateFindings](#) activa un evento Security Hub Findings - Imported.

En el caso de las cuentas de administrador, el feed de eventos EventBridge incluye eventos con las conclusiones tanto de su cuenta como de las cuentas de sus miembros.

En una región de agregación, el feed de eventos incluye eventos con los resultados de la región de agregación y las regiones vinculadas. Los hallazgos entre regiones se incluyen en el feed de eventos casi en tiempo real. Para obtener información sobre cómo configurar la agregación de resultados, consulte [Agregación de datos del CSPM en todas las regiones](#).

Puede definir reglas EventBridge que dirijan automáticamente los hallazgos a un flujo de trabajo de remediación, a una herramienta de terceros o a [otro EventBridge objetivo compatible](#). Las reglas pueden incluir filtros que solo apliquen la regla si el resultado tiene valores de atributo específicos.

Este método le permite enviar automáticamente todos los resultados ,o todos aquellos con determinadas características, a un flujo de trabajo de corrección o respuesta.

Consulte [the section called “Configuración de una regla EventBridge ”](#).

Resultados para acciones personalizadas (Security Hub Findings - Custom Action)

El CSPM de Security Hub también envía las conclusiones asociadas a acciones personalizadas a eventos EventBridge as Security Hub Findings - Custom Action.

Esto resulta útil para los analistas que trabajan con la consola CSPM de Security Hub y desean enviar un hallazgo específico, o un conjunto pequeño de hallazgos, a un flujo de trabajo de respuesta

o corrección. Puede seleccionar una acción personalizada para un máximo de 20 resultados a la vez. Cada hallazgo se envía EventBridge como un evento independiente. EventBridge

Al crear una acción personalizada, usted asigna un ID de acción personalizada. Puedes usar este identificador para crear una EventBridge regla que lleve a cabo una acción específica tras recibir un hallazgo asociado a ese identificador de acción personalizado.

Consulte [the section called “Configuración y uso de acciones personalizadas”](#).

Por ejemplo, puede crear una acción personalizada en Security Hub llamada CSPM. `send_to_ticketing` A continuación EventBridge, se crea una regla que se activa cuando se EventBridge recibe un resultado que incluye el identificador de la acción `send_to_ticketing` personalizada. La regla incluye lógica para enviar el resultado a su sistema de tickets. A continuación, puede seleccionar las conclusiones en Security Hub CSPM y utilizar la acción personalizada en Security Hub CSPM para enviar las conclusiones manualmente a su sistema de emisión de tickets.

Para ver ejemplos de cómo enviar las conclusiones del CSPM del Security Hub EventBridge para su posterior procesamiento, consulte [Cómo integrar las acciones personalizadas de AWS Security Hub Cloud Security Posture Management \(CSPM\) PagerDuty y Cómo habilitar las acciones personalizadas en Security Hub AWS Cloud Security Posture Management \(CSPM\) en el blog AWS Partner Network \(APN\)](#).

Resultados de Insight para acciones personalizadas (Security Hub Insight Results)

También puede utilizar acciones personalizadas para enviar conjuntos de información y resultados a eventos como eventos. EventBridge Security Hub Insight Results Los resultados de información son los recursos que coinciden con una información. Tenga en cuenta que cuando envía los resultados de la información a EventBridge, no envía los resultados a EventBridge. Solo está enviando los identificadores de recursos asociados a los resultados de información. Puede enviar hasta 100 identificadores de recursos a la vez.

De forma similar a las acciones personalizadas para los hallazgos, primero se crea la acción personalizada en Security Hub CSPM y, a continuación, se crea una regla en EventBridge

Consulte [the section called “Configuración y uso de acciones personalizadas”](#).

Por ejemplo, supongamos que ve un determinado resultado de información de interés que desea compartir con un colega. En ese caso, puede utilizar una acción personalizada para enviar ese resultado de información al colega a través de un chat o de un sistema de tickets.

EventBridge formatos de eventos para Security Hub CSPM

Los tipos de evento Security Hub Findings - Imported, Security Findings - Custom Action y Security Hub Insight Results utilizan los siguientes formatos de evento.

El formato del evento es el formato que se utiliza cuando el CSPM de Security Hub envía un evento. EventBridge

Security Hub Findings - Imported

Security Hub Findings - Importedeventos que se envían desde Security Hub CSPM para EventBridge usar el siguiente formato.

```
{
  "version": "0",
  "id": "CWE-event-id",
  "detail-type": "Security Hub Findings - Imported",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T21:52:17Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:securityhub:us-west-2::product/aws/maciek/arn:aws:maciek:us-west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/f2893b211841"
  ],
  "detail": {
    "findings": [
      <finding content>
    ]
  }
}
```

<finding content> es el contenido, en formato JSON, del resultado que envía el evento. Cada evento envía un único resultado.

Para obtener una lista completa de los atributos de los resultados, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

Para obtener información sobre cómo configurar EventBridge las reglas que se activan por estos eventos, consulte. [the section called “Configuración de una regla EventBridge ”](#)

Security Hub Findings - Custom Action

Security Hub Findings - Custom Action eventos que se envían desde Security Hub CSPM para EventBridge usar el siguiente formato. Cada resultado se envía en un evento independiente.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Findings - Custom Action",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
  ],
  "detail": {
    "actionName": "custom-action-name",
    "actionDescription": "description of the action",
    "findings": [
      {
        <finding content>
      }
    ]
  }
}
```

<finding content> es el contenido, en formato JSON, del resultado que envía el evento. Cada evento envía un único resultado.

Para obtener una lista completa de los atributos de los resultados, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

Para obtener información sobre cómo configurar EventBridge las reglas que se activan por estos eventos, consulte. [the section called “Configuración y uso de acciones personalizadas”](#)

Security Hub Insight Results

Security Hub Insight Resultseventos que se envían desde Security Hub CSPM para EventBridge usar el siguiente formato.

```
{
```



```

"version": "0",
"id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
"detail-type": "Security Hub Insight Results",
"source": "aws.securityhub",
"account": "111122223333",
"time": "2017-12-22T18:43:48Z",
"region": "us-west-1",
"resources": [
  "arn:aws:securityhub:us-west-1:111122223333::product/aws/maciek:us-west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
],
"detail": {
  "actionName": "name of the action",
  "actionDescription": "description of the action",
  "insightArn": "ARN of the insight",
  "insightName": "Name of the insight",
  "resultType": "ResourceAwsIamAccessKeyUserName",
  "number of results": "number of results, max of 100",
  "insightResults": [
    {"result 1": 5},
    {"result 2": 6}
  ]
}
}

```

Para obtener información sobre cómo crear una EventBridge regla que se active mediante estos eventos, consulte [the section called “Configuración y uso de acciones personalizadas”](#)

Configuración de una EventBridge regla para las conclusiones del CSPM de Security Hub

Puedes crear una regla en Amazon EventBridge que defina la acción que se debe realizar cuando se reciba un Security Hub Findings - Importedevento. Security Hub Findings - Importedlos eventos se desencadenan por las actualizaciones de [BatchUpdateFindings](#) las operaciones [BatchImportFindings](#).

Cada regla contiene un patrón de eventos, que identifica los eventos que activan la regla. El patrón de eventos siempre contiene la fuente del evento (`aws.securityhub`) y el tipo de evento (Resultados de Security Hub - Importado). El patrón de eventos también puede especificar filtros para identificar los resultados a los que se aplica la regla.

A continuación, la regla de eventos identifica los objetivos de la regla. Los objetivos son las acciones que se deben realizar cuando EventBridge recibe un evento de Security Hub Findings - Imported y el hallazgo coincide con los filtros.

Las instrucciones que se proporcionan aquí utilizan la EventBridge consola. Cuando utilizas la consola, crea EventBridge automáticamente la política basada en los recursos necesaria que permite EventBridge escribir en Amazon CloudWatch Logs.

También puede utilizar el [PutRule](#) funcionamiento de la EventBridge API. Sin embargo, si usa la EventBridge API, debe crear la política basada en recursos. Para obtener información sobre la política requerida, consulta [CloudWatch los permisos de registros](#) en la Guía del EventBridge usuario de Amazon.

Formato del patrón de eventos

El formato del patrón de eventos para los eventos Resultados de Security Hub - Importado es el siguiente:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source` identifica a Security Hub CSPM como el servicio que genera el evento.
- `detail-type` identifica el tipo de evento.
- `detail` es opcional y proporciona los valores de filtro para el patrón de eventos. Si el patrón de eventos no contiene un campo `detail`, todos los resultados activan la regla.

Puede filtrar los resultados en función de cualquier atributo del resultado. Para cada atributo, proporciona una matriz separada por comas de uno o más valores.

```
"<attribute name>": [ "<value1>", "<value2>" ]
```

Si proporciona más de un valor para un atributo, estos valores se unen mediante OR. Un resultado coincide con el filtro para un atributo individual si el resultado tiene cualquiera de los valores enumerados. Por ejemplo, si proporciona INFORMATIONAL y LOW como valores para Severity.Label, entonces el resultado coincide si tiene una etiqueta de gravedad de INFORMATIONAL o LOW.

Los atributos se unen mediante AND. Un resultado coincide si este coincide con los criterios de filtrado para todos los atributos proporcionados.

Al proporcionar un valor de atributo, debe reflejar la ubicación de ese atributo dentro de la estructura del formato de búsqueda AWS de seguridad (ASFF).

Tip

Para filtrar los resultados de los controles, le recomendamos que utilice los [campos ASFF](#) SecurityControlId o SecurityControlArn como filtros, en vez de Title o Description. Estos últimos campos podrían cambiar ocasionalmente, mientras que el ID de control y el ARN son identificadores estáticos.

En el siguiente ejemplo, el patrón de eventos proporciona valores de filtro para ProductArn y Severity.Label, por lo que un resultado coincide si lo genera Amazon Inspector y tiene una etiqueta de gravedad de INFORMATIONAL o LOW.

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
      "Severity": {
        "Label": ["INFORMATIONAL", "LOW"]
      }
    }
  }
}
```

```
}  
}
```

Creación de una regla de eventos

Puede utilizar un patrón de eventos predefinido o un patrón de eventos personalizado para crear una regla. EventBridge Si selecciona un patrón predefinido, rellena EventBridge automáticamente `source` y `detail-type`. EventBridge también proporciona campos para especificar los valores de filtro para los siguientes atributos de búsqueda:

- `AwsAccountId`
- `Compliance.Status`
- `Criticality`
- `ProductArn`
- `RecordState`
- `ResourceId`
- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

Para crear una EventBridge regla (consola)

1. Abra la EventBridge consola de Amazon en <https://console.aws.amazon.com/events/>.
2. Con los siguientes valores, cree una EventBridge regla que supervise la búsqueda de eventos:
 - En Tipo de regla, seleccione Regla con un patrón de evento.
 - Elija cómo crear el patrón de eventos.

Cómo crear el patrón de eventos con...	Haga lo siguiente...
Una plantilla	En la sección Patrón de eventos, elija una de las siguientes opciones:

Cómo crear el patrón de eventos con...	Haga lo siguiente...	
	• En Origen del evento, seleccione Servicios de AWS . • En Servicio de AWS , elija Security Hub. • En Tipo de evento, seleccione Resultados de Security Hub - Importado. • (Opcional) Para que la regla sea más específica, agregue valores de filtro. Por ejemplo, para limitar la regla a resultados con estados de registro activos, en Estados de registro específicos, seleccione Activo.	

Cómo crear el patrón de eventos con...	Haga lo siguiente...	
Un patrón de eventos personalizado (Utilice un patrón personalizado si desea filtrar los resultados en función de atributos que no aparecen en la EventBridge consola).	- En la sección Patrón de evento, seleccione Patrones personalizados (editor JSON) y luego pegue el siguiente patrón de evento en el área de texto: <pre data-bbox="690 630 1063 1428"> { "source": ["aws.secu rityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "<attribut e name> ": ["<value1>", "<value2>"] } } }</pre> - Actualice el patrón de eventos para incluir el atributo y los valores del atributo que desee utilizar como filtro. Por ejemplo, para aplicar la regla a los resultados que tengan un estado de	

Cómo crear el patrón de eventos con...	Haga lo siguiente...	
	verificación TRUE_POSITIVE , utilice el siguiente patrón de ejemplo: <pre data-bbox="690 430 1063 1186"> { "source": ["aws.secu rityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "Verifica tionState": ["TRUE_POSITIVE"] } } }</pre>	

- Para los tipos de destino, elija el AWS servicio y, para Seleccione un objetivo, elija un objetivo, como un tema o AWS Lambda una función de Amazon SNS. El destino se activa cuando se recibe un evento que coincide con el patrón de eventos definido en la regla.

Para obtener más información sobre la creación de reglas, consulta [Cómo crear EventBridge reglas de Amazon que reaccionen a los eventos](#) en la Guía del EventBridge usuario de Amazon.

Utilizar acciones personalizadas para enviar las conclusiones y los resultados de información a EventBridge

Para usar las acciones personalizadas de AWS Security Hub Cloud Security Posture Management (CSPM) para enviar hallazgos o información a Amazon EventBridge, primero debe crear la acción

personalizada en Security Hub CSPM. A continuación, puede definir las reglas EventBridge que se apliquen a sus acciones personalizadas.

Puede crear hasta 50 acciones personalizadas.

Si habilita la agregación entre regiones y administra los resultados desde la región de agregación, debe crear acciones personalizadas en la región de agregación.

La regla en EventBridge utiliza el nombre de recurso de Amazon (ARN) de la acción personalizada.

Crear una acción personalizada

Al crear una acción personalizada en AWS Security Hub Cloud Security Posture Management (CSPM), se especifica su nombre, descripción y un identificador único.

Una acción personalizada especifica qué acciones se deben realizar cuando un EventBridge evento coincide con una EventBridge regla. Security Hub CSPM envía cada hallazgo EventBridge como un evento.

Elija su método preferido y siga los pasos para crear una acción personalizada.

Console

Para crear una acción personalizada en Security Hub CSPM (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Settings (Configuración) y luego elija Custom actions (Acciones personalizadas).
3. Seleccione Create custom action (Crear acción personalizada).
4. Proporcione un Name (Nombre), Description (Descripción) e Custom action ID (ID de acción personalizada) para la acción.

El Name (Nombre) debe tener menos de 20 caracteres.

El ID de acción personalizada debe ser único por cada cuenta de AWS .

5. Seleccione Create custom action (Crear acción personalizada).
6. Anote el ARN de acción personalizada. Debe usar el ARN cuando cree una regla para asociarla con esta acción en EventBridge.

API

Para crear una acción personalizada (API)

Utilice la operación [CreateActionTarget](#). Si está utilizando el AWS CLI, ejecute el [create-action-target](#) comando.

En el siguiente ejemplo, se crea una acción personalizada para enviar resultados a una herramienta de corrección. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub create-action-target --name "Send to remediation" --description "Action to send the finding for remediation tracking" --id "Remediation"
```

Definir una regla en EventBridge

Para activar una acción personalizada en Amazon EventBridge, debes crear la regla correspondiente en EventBridge. La definición de la regla incluye el nombre de recurso de Amazon (ARN) de la acción personalizada.

El patrón de evento para un evento Resultados de Security Hub - Acción personalizada tiene el siguiente formato:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

El patrón de evento para un evento Resultados de Security Hub - Acción personalizada tiene el siguiente formato:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
```

```
"Security Hub Insight Results"
],
"resources": [ "<custom action ARN>" ]
}
```

En ambos patrones, *<custom action ARN>* es el ARN de una acción personalizada. Puede configurar una regla que se aplique a más de una acción personalizada.

Las instrucciones que se proporcionan aquí son para la EventBridge consola. Al utilizar la consola, crea EventBridge automáticamente la política basada en los recursos necesaria que permite EventBridge escribir CloudWatch en los registros.

También puedes usar la operación de [PutRule](#) API de la EventBridge API. Sin embargo, si usa la EventBridge API, debe crear la política basada en recursos. Para obtener más información sobre la política requerida, consulta [CloudWatch los permisos de registros](#) en la Guía del EventBridge usuario de Amazon.

Para definir una regla en EventBridge (EventBridge consola)

1. Abre la EventBridge consola de Amazon 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.
5. En Bus de eventos, elija el bus de eventos que desea asociar a esta regla. Si desea que esta regla coincida con eventos procedentes de su cuenta, seleccione predeterminado. Cuando un servicio de AWS en la cuenta emite un evento, siempre va al bus de eventos predeterminado de la cuenta.
6. En Tipo de regla, seleccione Regla con un patrón de eventos.
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 del evento, seleccione Servicios de AWS .
11. En Servicio de AWS , seleccione Security Hub.
12. En Tipo de evento, realice una de las siguientes operaciones:
 - Para crear una regla que se aplique al enviar resultados a una acción personalizada, seleccione Resultados de Security Hub - Acción personalizada.

- Para crear una regla que se aplique al enviar resultados de información a una acción personalizada, seleccione Resultados de información de Security Hub.

13. Elija Acción personalizada específica ARNs y añada un ARN de acción personalizada.

Si la regla se aplica a varias acciones personalizadas, selecciona Añadir para añadir más acciones ARNs personalizadas.

14. Elija Siguiente.

15. En Seleccionar objetivos, elija y configure el objetivo por invocar cuando esta regla coincida.

16. Elija Siguiente.

17. (Opcional) Introduzca una o varias etiquetas para la regla. Para obtener más información, consulta las [EventBridge etiquetas de Amazon](#) en la Guía del EventBridge usuario de Amazon.

18. Elija Siguiente.

19. Revise los detalles de la regla y seleccione Creación de regla.

Cuando realizas una acción personalizada sobre los hallazgos o los resultados de información de tu cuenta, los eventos se generan en EventBridge.

Selección de una acción personalizada para resultados y resultados de información

Después de crear las acciones personalizadas de AWS Security Hub Cloud Security Posture Management (CSPM) y las EventBridge reglas de Amazon, puede enviar las conclusiones y los resultados de información EventBridge para su administración y procesamiento automáticos.

Los eventos se envían EventBridge únicamente a la cuenta en la que se visualizan. Si consulta un hallazgo con una cuenta de administrador, el evento se envía a EventBridge la cuenta de administrador.

Para que las llamadas a las AWS API sean efectivas, las implementaciones del código de destino deben cambiar de rol a cuentas de miembros. Esto también significa que el rol al que se cambia debe implementarse en cada miembro en el que sea necesario actuar.

Para enviar los resultados a EventBridge (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en <https://console.aws.amazon.com/securityhub/>
2. Visualice una lista de resultados:

- En Resultados, puede ver los resultados de todas las integraciones de productos y controles habilitados.
 - En Estándares de seguridad, puede dirigirse a una lista de resultados generados a partir de un control específico. Para obtener más información, consulte [Revisión de los detalles de los controles en Security Hub \(CSPM\)](#).
 - En Integraciones puede dirigirse a una lista de resultados generada por una de las integraciones habilitadas. Para obtener más información, consulte [Visualización de los resultados de una integración de Security Hub \(CSPM\)](#).
 - En Información, puede dirigirse a una lista de resultados de un resultado de información. Para obtener más información, consulte [Revisión de los conocimientos del Security Hub \(CSPM\) y adopción de medidas en función de ellos](#).
3. Seleccione los resultados a los que desee enviarlos. EventBridge Puede seleccionar hasta 20 hallazgos a la vez.
 4. En Acciones, elija la acción personalizada que se ajuste a la EventBridge regla que desee aplicar.

El CSPM de Security Hub envía un evento Security Hub Findings - Custom Action independiente para cada hallazgo.

Para enviar los resultados de las estadísticas a EventBridge (consola)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Insights.
3. En la página Estadísticas, elija la información que incluye los resultados a los que desea enviarlos. EventBridge
4. Seleccione los resultados de la información a la que desee enviarlos EventBridge. Puede seleccionar hasta 20 resultados a la vez.
5. En Acciones, elija la acción personalizada que se ajuste a la EventBridge regla que desee aplicar.

Trabajar con el panel de control de Security Hub CSPM

La página Resumen de la consola de Security Hub muestra un resumen de los riesgos, las secuencias de ataque y la cobertura de seguridad. Esta página le ayuda a identificar los riesgos y las secuencias de ataque en función de su gravedad y de la cobertura de las distintas capacidades de seguridad. Puede personalizar esta página añadiendo y quitando distintos widgets de seguridad y estableciendo criterios de filtrado para recuperar tipos de datos específicos.

Las personalizaciones de esta página se guardan para usarlas en el futuro. Si los usuarios de su cuenta personalizan esta página, sus preferencias de personalización se guardan independientemente de las suyas.

Si su cuenta es la cuenta de administrador delegado de una organización, los datos incluyen los resultados de su cuenta y de las cuentas de los miembros. Si su cuenta es una cuenta de miembro o una cuenta independiente, los datos solo incluyen los hallazgos de su cuenta.

Si configura la agregación entre regiones en Security Hub (CSPM), en esta página se muestran los resultados de la agregación.

Note

Cada vez que abra esta página, se actualizará automáticamente. Sin embargo, las puntuaciones de seguridad y los estados de control se actualizan cada 24 horas.

El widget de resumen de riesgos

Este widget muestra todos los riesgos en función de su gravedad. Los riesgos con mayor gravedad aparecen primero. Los riesgos se basan en un análisis de los hallazgos y características de Security Hub, CSPM y otros. Servicios de AWS

El widget de resumen de amenazas

Este widget muestra todas las secuencias de ataque en función de la gravedad. Las secuencias de ataque con mayor gravedad aparecen primero. Las secuencias de ataque están relacionadas con una serie de eventos e identifican las posibles amenazas en su entorno. También se originan en GuardDuty.

El widget de cobertura de seguridad

Widgets disponibles para el panel Resumen

El panel de resumen incluye widgets que reflejan el panorama moderno de amenazas a la seguridad en la nube, guiados por las operaciones de seguridad y las experiencias de AWS los clientes. Algunos widgets se muestran de forma predeterminada, mientras que otros no. Puede agregar o quitar widgets para personalizar la vista del panel.

Para agregarlos, seleccione Agregar widget en la parte superior derecha de la página Resumen. En la barra de búsqueda, ingrese el título del widget. Arrastre y suelte el widget en el panel.

Widgets mostrados de forma predeterminada

El panel Resumen incluye los siguientes widgets de forma predeterminada:

Principales secuencias de amenazas

Muestra las secuencias de amenazas de mayor gravedad. Los hallazgos de secuencias de amenazas, conocidos como hallazgos de secuencias de ataques en Amazon GuardDuty, correlacionan varios eventos para identificar posibles amenazas para su AWS entorno. Las secuencias de amenazas pueden incluir comportamientos de ataque recientes o en curso (dentro de un período de 24 horas) en su entorno, lo que a su vez puede suponer un mayor riesgo. Debe tener GuardDuty activada la protección GuardDuty S3 para recibir hallazgos de secuencias de amenazas en Security Hub CSPM.

Principales riesgos

Muestra un resumen de los principales riesgos de su entorno. La parte superior del widget muestra el recuento de riesgos en cada nivel de gravedad. Puede elegir un nivel de gravedad para ir a la página de riesgos y filtrar los riesgos según el nivel de gravedad seleccionado. Los riesgos que más se producen en su entorno aparecen primero. Este widget le ayuda a priorizar los riesgos que se deben mitigar.

Cobertura de seguridad

Resume el alcance de su cobertura de seguridad en función de los resultados del control de cobertura. Los controles de cobertura comprueban si un Servicio de AWS producto específico y sus capacidades están habilitadas (por ejemplo, [\[Macie.1\] Amazon Macie debe estar habilitado](#)).

Este widget te ayuda a asegurarte de que tienes información PASSED sobre los controles de cobertura. La consola CSPM de Security Hub proporciona enlaces desde este widget para ayudarle a activar las capacidades de seguridad que faltan. Recomendamos utilizar una configuración central para habilitar las capacidades de seguridad que faltan en varias Cuentas de AWS y Regiones de AWS. Para obtener más información, consulte [Descripción de la configuración central en Security Hub \(CSPM\)](#).

Estándares de seguridad

Muestra tu puntuación de seguridad resumida más reciente y la puntuación de seguridad de cada estándar CSPM de Security Hub. Las puntuaciones de seguridad, que van del 0 % al 100 %, representan la proporción de controles aprobados en relación con todos los controles habilitados. Para obtener más información acerca de estas puntuaciones, consulte [Método de cálculo de las puntuaciones de seguridad](#). Este widget le ayuda a entender su postura general en materia de seguridad.

Estándares de seguridad

Muestra tu puntuación de seguridad resumida más reciente y la puntuación de seguridad de cada estándar CSPM de Security Hub. Las puntuaciones de seguridad, que van del 0 % al 100 %, representan la proporción de controles aprobados en relación con todos los controles habilitados. Para obtener más información acerca de estas puntuaciones, consulte [Método de cálculo de las puntuaciones de seguridad](#). Este widget le ayuda a entender su postura general en materia de seguridad.

Los activos con más resultados

Proporciona información general de los activos, las cuentas y las aplicaciones que generan más resultados. La lista se ordena por número de resultados de forma descendente. En el widget, cada pestaña muestra los seis elementos principales de esa categoría, agrupados por gravedad y tipo de recurso. Si elige un número en la columna Resultados totales, Security Hub CSPM abre una página que muestra los hallazgos del activo. Este widget le ayuda a identificar rápidamente cuáles de sus activos principales presentan posibles amenazas a la seguridad.

Resultados por región

Muestra el número total de hallazgos, agrupados por gravedad, en cada uno de los casos Región de AWS en los que Security Hub CSPM está activado. Este widget le ayuda a identificar los problemas de seguridad que pueden afectar a determinadas regiones. Si abre el panel en su región de agregación, este widget le ayudará a supervisar los posibles problemas de seguridad de cada región vinculada.

Tipos de amenazas más comunes

Proporciona un desglose de los 10 tipos de amenazas más comunes en su AWS entorno. Esto incluye amenazas como derivación de privilegios, uso de credenciales expuestas o comunicación con direcciones IP maliciosas.

Para ver estos datos, [Amazon GuardDuty](#) debe estar activado. Si es así, elige un tipo de amenaza en este widget para abrir la GuardDuty consola y revisar los resultados relacionados con esta amenaza. Este widget le ayuda a evaluar las posibles amenazas en el contexto de otros problemas de seguridad.

Vulnerabilidades de software con exploits

Proporciona un resumen de las vulnerabilidades de software que existen en su AWS entorno y que presentan vulnerabilidades conocidas. También puede revisar un desglose de las vulnerabilidades que tienen soluciones disponibles y las que no.

Para ver estos datos, [Amazon Inspector](#) debe estar habilitado. Si es así, seleccione una estadística en este widget para abrir la consola de Amazon Inspector y ver más detalles sobre la vulnerabilidad. Este widget le ayuda a evaluar las vulnerabilidades del software en el contexto de otros problemas de seguridad.

Nuevos resultados a lo largo del tiempo

Muestra las tendencias en el número de nuevos resultados diarios durante los últimos 90 días. Puede desglosar los datos por gravedad o por proveedor para obtener un contexto adicional. Este widget le ayuda a saber si ha aumentado o disminuido el volumen de resultados en momentos específicos durante los últimos 90 días.

Recursos con la mayor cantidad de resultados

Proporciona un resumen de los recursos que han generado más resultados, desglosados por los siguientes tipos de recursos: depósitos de Amazon Simple Storage Service (Amazon S3), instancias AWS Lambda de Amazon Elastic Compute Cloud (EC2Amazon) y funciones.

En el widget, cada pestaña se centra en uno de los tipos de recursos anteriores y enumera las 10 instancias de recursos que han generado la mayoría de los resultados. Para revisar los resultados de un recurso específico, seleccione la instancia del recurso. Este widget le ayuda a clasificar los hallazgos de seguridad asociados a recursos comunes AWS .

Widgets ocultos de forma predeterminada

Los siguientes widgets también están disponibles en el panel Resumen, pero se han ocultado de forma predeterminada:

AMIs con la mayor cantidad de hallazgos

Proporciona una lista de las 10 Amazon Machine Images (AMIs) que han generado más resultados. Estos datos solo están disponibles si Amazon los EC2 ha habilitado para tu cuenta. Le ayuda a identificar cuáles AMIs representan posibles riesgos de seguridad.

Entidades principales de IAM con la mayor cantidad de resultados

Proporciona una lista de los 10 usuarios AWS Identity and Access Management (IAM) que han generado más hallazgos. Este widget le ayuda a llevar a cabo tareas administrativas y de facturación. Muestra qué usuarios contribuyen más al uso del CSPM de Security Hub.

Cuentas con la mayor cantidad de resultados (por gravedad)

Muestra un gráfico de las 10 cuentas que han generado la mayor cantidad de resultados, agrupadas por gravedad. Este widget le ayuda a determinar en qué cuentas debe centrar los esfuerzos de análisis y corrección.

Cuentas con la mayor cantidad de resultados (por tipo de recurso)

Muestra un gráfico de las 10 cuentas que han generado la mayor cantidad de resultados, agrupadas por tipo de recurso. Este widget le ayuda a determinar qué cuentas y tipos de recursos se deben priorizar en cuestión de análisis y corrección.

Información

Enumera cinco [conocimientos gestionados por CSPM de Security Hub](#) y el número de hallazgos que generaron. Dichos elementos identifican un área de seguridad específica que requiere atención.

Los últimos hallazgos de las integraciones AWS

[Muestra el número de hallazgos que recibió en Security Hub CSPM desde Integrated. Servicios de AWS](#) También muestra cuándo recibió por última vez los resultados de cada servicio integrado. Este widget proporciona datos de hallazgos consolidados de varios. Servicios de AWS Para obtener más detalles, seleccione un servicio integrado. A continuación, Security Hub CSPM abre la consola de ese servicio.

Filtrar el panel de resumen en Security Hub CSPM

Puede seleccionar el panel de resumen de la consola AWS Security Hub Cloud Security Posture Management (CSPM) para que incluya solo los datos de seguridad que sean más relevantes para usted. Por ejemplo, si es miembro de un equipo de aplicaciones, puede crear una vista específica para una aplicación crítica de su entorno de producción. Si es miembro de un equipo de seguridad, puede crear una vista específica que le ayude a centrarse en los resultados de mayor gravedad.

Para crear estas vistas seleccionadas, ingrese los criterios de filtro en el cuadro de filtrado encima del panel. Si aplica criterios de filtro, estos se aplican a todos los datos y widgets del panel, excepto a los datos de los widgets de Información y Estándares de seguridad. Para ver una lista de los widgets disponibles en el panel de control, consulte [Widgets disponibles para el panel Resumen](#).

Puede filtrar los datos mediante los campos siguientes:

- Nombre de cuenta
- ID de cuenta
- Nombre de recurso de Amazon (ARN) de aplicaciones
- Nombre de la aplicación
- Nombre del producto (para un producto Servicio de AWS o un producto de terceros que envía los resultados a Security Hub CSPM)
- Record state (Estado de registro)
- Región
- Etiqueta de recurso
- Gravedad
- Estado del flujo de trabajo

Los datos del panel se filtran, de forma predeterminada, según los siguientes criterios:

`Workflow.Status` es NOTIFIED o NEW, y `RecordState` es ACTIVE. Estos criterios aparecen encima del panel, debajo del cuadro de filtro. Para eliminar estos criterios, seleccione X en el token del filtro para los criterios que desea eliminar.

Si aplica criterios de filtro que desea volver a utilizar, puede guardarlos como un conjunto de filtros. Un conjunto de filtros es una agrupación de criterios de filtro que crea y guarda para volver a aplicarlos al revisar los datos que se muestran en el panel Resumen.

 Note

Los siguientes campos no se pueden guardar como parte de un conjunto de filtros: ARN de aplicación, nombre de aplicación y etiqueta de recurso.

Creación y almacenamiento de conjuntos de filtros

Para crear y guardar un conjunto de filtros, siga estos pasos.

Creación y almacenamiento de un conjunto de filtros

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Resumen.
3. En el cuadro de filtros situado encima del panel Resumen, ingrese los criterios de filtro para el conjunto correspondiente.
4. En el menú Borrar filtros, seleccione Guardar nuevo conjunto de filtros.
5. En el cuadro de diálogo Guardar conjunto de filtros, ingrese un nombre para el conjunto de filtros.
6. (Opcional) Para utilizar el conjunto de filtros predeterminado cada vez que abra la página Resumen, seleccione la opción para establecerlo como vista predeterminada.
7. Seleccione Save.

Para cambiar entre los conjuntos de filtros que ha creado y guardado, utilice el menú Seleccionar un conjunto de filtros situado encima del panel Resumen. Al seleccionar un conjunto de filtros, Security Hub CSPM aplica los criterios del conjunto de filtros a los datos del panel.

Actualización o eliminación de conjuntos de filtros

Siga estos pasos para actualizar o eliminar un conjunto de filtros existente. Si elimina un conjunto de filtros que está configurado actualmente como vista predeterminada del panel Resumen, la vista predeterminada se restablece a la vista CSPM predeterminada de Security Hub.

Actualización o eliminación de un conjunto de filtros

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Resumen.
3. En el menú Seleccionar un conjunto de filtros situado encima de la página Resumen, seleccione el conjunto de filtros.
4. En el menú Borrar filtros, haga una de las siguientes operaciones:
 - Para actualizar el conjunto de filtros, seleccione Actualizar conjunto de filtros actual. A continuación, ingrese sus cambios en el cuadro de diálogo que aparece.
 - Para eliminar el conjunto de filtros, seleccione Eliminar conjunto de filtros actual. A continuación, en el cuadro de diálogo que aparece, seleccione Eliminar.

Personalización del panel de resumen en Security Hub (CSPM)

Puede personalizar el panel de resumen de la consola AWS Security Hub Cloud Security Posture Management (CSPM) de varias maneras. Por ejemplo, puede agregar y eliminar widgets del panel. También puede reorganizar y cambiar el tamaño de los widgets del panel. Para ver una lista de los widgets disponibles en el panel de control, consulte [Widgets disponibles para el panel Resumen](#).

Si personaliza el panel, Security Hub CSPM aplicará los cambios inmediatamente y guardará la nueva configuración del panel. Los cambios se aplican a la vista del panel de control en todos los navegadores Regiones de AWS y navegadores.

Personalización del panel Resumen

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, elija Resumen.
3. Realice uno de los siguientes procedimientos:
 - Para agregar un widget, seleccione Agregar widgets en la esquina superior derecha de la página. En la barra de búsqueda, ingrese el título del widget que desea agregar. A continuación, arrastre el widget a la ubicación que desee.
 - Para eliminar un widget, seleccione los tres puntos que aparecen en la esquina superior derecha del widget.

- Para mover un widget, seleccione el controlador que está en su esquina superior izquierda y, a continuación, arrastre el widget a la ubicación que desee.
- Para cambiar el tamaño de un widget, elija el controlador de cambio de tamaño que está en su esquina inferior derecha. Arrastre el borde del widget hasta que tenga el tamaño que prefiera.

Para restaurar posteriormente la configuración original, seleccione Restablecer al diseño predeterminado en la parte superior de la página.

Límites regionales para Security Hub CSPM

Algunas funciones AWS de Security Hub Cloud Security Posture Management (CSPM) solo están disponibles en algunas. Regiones de AWS En las siguientes secciones se especifican estos límites regionales. Para obtener una lista completa de todas las regiones en las que Security Hub CSPM está disponible actualmente, consulte los [puntos finales y las cuotas de AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) en el. Referencia general de AWS

Restricciones de agregación entre regiones

En AWS GovCloud (US) las regiones, [la agregación entre regiones solo](#) está disponible para los resultados, las actualizaciones de las búsquedas y la información de todas las regiones. AWS GovCloud (US) En concreto, solo puede agregar los hallazgos, las actualizaciones y la información entre AWS GovCloud (EE. UU. este) y (EE. UU., oeste). AWS GovCloud

En las regiones de China, la agregación entre regiones solo está disponible para los resultados, las actualizaciones de resultados y los hallazgos de las regiones de China. En concreto, solo puede agregar resultados, actualizaciones de resultados y hallazgos entre China (Pekín) y China (Ningxia).

No puede usar una región que esté deshabilitada de forma predeterminada como región de agregación. Para ver una lista de las regiones que están deshabilitadas de forma predeterminada, consulta la [sección Habilitar o deshabilitar Regiones de AWS tu cuenta](#) en la Guía de AWS Account Management referencia.

Disponibilidad de las integraciones por región

Algunas integraciones no están disponibles en todas las regiones. Si una integración no está disponible en una región específica, no aparece en la página Integraciones de la consola CSPM de Security Hub al elegir esa región.

Integraciones compatibles en las regiones de China (Pekín) y China (Ningxia)

Las regiones de China (Pekín) y China (Ningxia) solo admiten las siguientes [integraciones con AWS servicios](#):

- AWS Firewall Manager

- Amazon GuardDuty
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer
- AWS Systems Manager OpsCenter
- AWS Systems Manager Administrador de parches

Las regiones de China (Pekín) y China (Ningxia) solo admiten las siguientes [integraciones de terceros](#):

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar
- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler
- RSA Archer
- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

Integraciones compatibles en las regiones (EE. UU. este) y AWS GovCloud
AWS GovCloud (EE. UU., oeste)

[Las regiones AWS GovCloud \(EE. UU. Este\) y AWS GovCloud \(EE. UU. Oeste\) solo admiten las siguientes integraciones con servicios: AWS](#)

- AWS Config
- Amazon Detective

- AWS Firewall Manager
- Amazon GuardDuty
- AWS Health
- Analizador de acceso de IAM
- Amazon Inspector
- AWS IoT Device Defender

Las regiones AWS GovCloud (EE. UU. Este) y AWS GovCloud (EE. UU. Oeste) solo admiten las siguientes integraciones [de terceros](#):

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud
- Atlassian OpsGenie
- Caveonix Cloud
- Cloud Custodian
- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB
- Forcepoint DLP
- Forcepoint NGFW
- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator
- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series(disponible solo en (EE. UU. Oeste AWS GovCloud))
- Prowler
- Rackspace Technology – Cloud Native Security

- Rapid7 InsightConnect
- RSA Archer
- SecureCloudDb
- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

Disponibilidad de los estándares por región

El estándar AWS Control Tower de administración de servicios solo está disponible en las regiones AWS Control Tower compatibles, incluidas las regiones. AWS GovCloud (US) Para ver una lista de las regiones compatibles AWS Control Tower actualmente, consulta [Cómo Regiones de AWS trabajar con](#) ellas AWS Control Tower en la Guía del AWS Control Tower usuario.

El estándar AWS de etiquetado de recursos no está disponible en el oeste de Canadá (Calgary), China y las regiones. AWS GovCloud (US)

Hay otros estándares de seguridad disponibles en todas las regiones en las que Security Hub CSPM está disponible actualmente.

Disponibilidad de los controles por región

Algunos controles CSPM de Security Hub no están disponibles en todas las regiones. Para ver una lista de los controles que no están disponibles en cada región, consulte. [Límites regionales de los controles CSPM de Security Hub](#)

En la consola CSPM de Security Hub, un control no aparece en la lista de controles si no está disponible en la región en la que ha iniciado sesión actualmente. La excepción es una región de agregación. Si configura una región de agregación e inicia sesión en esa región, la consola muestra los controles que están disponibles en la región de agregación o en una o más regiones vinculadas.

Límites regionales de los controles CSPM de Security Hub

Algunos controles AWS de Security Hub Cloud Security Posture Management (CSPM) no están disponibles en todos. Regiones de AWS En esta página, se especifican los controles que no están disponibles en regiones específicas.

En la consola CSPM de Security Hub, un control no aparece en la lista de controles si no está disponible en la región en la que ha iniciado sesión actualmente. La excepción es una región de agregación. Si configura una región de agregación e inicia sesión en esa región, la consola muestra los controles que están disponibles en la región de agregación o en una o más regiones vinculadas.

Regiones de AWS

- [Este de EE. UU. \(Norte de Virginia\)](#)
- [Este de EE. UU. \(Ohio\)](#)
- [Oeste de EE. UU. \(Norte de California\)](#)
- [Oeste de EE. UU. \(Oregón\)](#)
- [África \(Ciudad del Cabo\)](#)
- [Asia-Pacífico \(Hong Kong\)](#)
- [Asia-Pacífico \(Hyderabad\)](#)
- [Asia-Pacífico \(Yakarta\)](#)
- [Asia-Pacífico \(Malasia\)](#)
- [Asia-Pacífico \(Melbourne\)](#)
- [Asia-Pacífico \(Bombay\)](#)
- [Asia-Pacífico \(Osaka\)](#)
- [Asia-Pacífico \(Seúl\)](#)
- [Asia-Pacífico \(Singapur\)](#)
- [Asia-Pacífico \(Sídney\)](#)
- [Asia-Pacífico \(Tailandia\)](#)
- [Asia-Pacífico \(Tokio\)](#)
- [Canadá \(centro\)](#)
- [Oeste de Canadá \(Calgary\)](#)
- [China \(Pekín\)](#)
- [China \(Ningxia\)](#)
- [Europa \(Fráncfort\)](#)
- [Europa \(Irlanda\)](#)
- [Europa \(Londres\)](#)
- [Europa \(Milán\)](#)

- [Europa \(París\)](#)
- [Europa \(España\)](#)
- [Europa \(Estocolmo\)](#)
- [Europa \(Zúrich\)](#)
- [Israel \(Tel Aviv\)](#)
- [México \(central\)](#)
- [Medio Oriente \(Baréin\)](#)
- [Medio Oriente \(EAU\)](#)
- [América del Sur \(São Paulo\)](#)
- [AWS GovCloud \(Este de EE. UU.\)](#)
- [AWS GovCloud \(EEUU-Oeste\)](#)

Este de EE. UU. (Norte de Virginia)

Los siguientes controles no se admiten en la región EE.UU. Este (Virginia del Norte).

- [\[ElastiCache.4\]](#) los grupos de ElastiCache replicación deben estar cifrados en reposo
- [\[ElastiCache.5\]](#) los grupos de ElastiCache replicación deben cifrarse en tránsito
- [\[ElastiCache.6\]](#) Los grupos de replicación ElastiCache (Redis OSS) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS
- [\[ElastiCache.7\]](#) los ElastiCache clústeres no deben usar el grupo de subredes predeterminado
- [\[GlobalAccelerator.1\]](#) Los aceleradores de Global Accelerator deben estar etiquetados
- [\[S3.24\]](#) Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público

Este de EE. UU. (Ohio)

Los siguientes controles no se admiten en la región EE.UU. Este (Ohio).

- [\[AppSync.1\]](#) Las cachés de las AWS AppSync API deben cifrarse en reposo
- [\[AppSync.6\]](#) Las cachés de las AWS AppSync API deben cifrarse en tránsito
- [\[CloudFront.1\]](#) CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado

- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[EC2.224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IoT Twin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Twin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoT Wireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)

- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

Oeste de EE. UU. (Norte de California)

Los siguientes controles no se admiten en la región EE.UU. Oeste (Norte de California).

- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)

- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DocumentDb.6\] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)

- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[IoT Events .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoT Events .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Events .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Site Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Site Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Twin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoT Wireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

- [\[WorkSpaces.1\]](#) los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [\[WorkSpaces.2\]](#) los volúmenes WorkSpaces raíz deben cifrarse en reposo

Oeste de EE. UU. (Oregón)

Los siguientes controles no se admiten en la región EE.UU. Oeste (Oregón).

- [\[AppSync.1\]](#) Las cachés de las AWS AppSync API deben cifrarse en reposo
- [\[AppSync.6\]](#) Las cachés de las AWS AppSync API deben cifrarse en tránsito
- [\[CloudFront.1\]](#) CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [\[CloudFront.3\]](#) CloudFront las distribuciones deben requerir el cifrado en tránsito
- [\[CloudFront.4\]](#) CloudFront Las distribuciones deben tener configurada la conmutación por error de origen
- [\[CloudFront.5\]](#) CloudFront las distribuciones deben tener el registro habilitado
- [\[CloudFront.6\]](#) CloudFront Las distribuciones deben tener WAF habilitado
- [\[CloudFront.7\]](#) CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados
- [\[CloudFront.8\]](#) CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS
- [\[CloudFront.9\]](#) CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados
- [\[CloudFront.10\]](#) CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados
- [\[CloudFront.12\]](#) CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes
- [\[CloudFront.13\]](#) CloudFront Las distribuciones deben usar el control de acceso de origen
- [\[CloudFront.14\]](#) CloudFront Las distribuciones deben etiquetarse
- [\[EC2.173\]](#) Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [\[ECR.4\]](#) Los repositorios públicos de ECR deben estar etiquetados
- [\[IAM.26\]](#) Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse
- [\[Route53.1\]](#) Las comprobaciones de estado de Route 53 deben estar etiquetadas
- [Las zonas alojadas públicas de Route 53 \[Route53.2\]](#) deben registrar las consultas de DNS
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\]](#) debe estar habilitado
- [Las reglas globales de \[WAF.6\]](#) AWS WAF clásicas deben tener al menos una condición

- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

África (Ciudad del Cabo)

Los siguientes controles no se admiten en la región de África (Ciudad del Cabo).

- [\[Amplify.1\] Las aplicaciones de Amplify deben estar etiquetadas](#)
- [\[Amplify.2\] Las ramas de Amplify deben estar etiquetadas](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)

- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Cognito.1\] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DocumentDb.6\] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC24\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.8\] EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancias IMDSv2](#)
- [\[EC2.14\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 o: :/0 al puerto 3389](#)
- [\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.177\] las sesiones espejo EC2 de tráfico deberían estar etiquetadas](#)
- [\[EC2.179\] Los objetivos EC2 de tráfico reflejados deben estar etiquetados](#)

- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[ELB.2\] Los equilibradores de carga clásicos con agentes de escucha SSL/HTTPS deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ES.3\] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [Los perfiles de AWS IoT Device Defender seguridad \[IoT.1\] deben estar etiquetados](#)
- [\[IoT.2\] las acciones de AWS IoT Core mitigación deben estar etiquetadas](#)
- [AWS IoT Core Las dimensiones de \[IoT.3\] deben estar etiquetadas](#)
- [Los AWS IoT Core autorizadores \[IoT.4\] deben estar etiquetados](#)
- [Los alias de los AWS IoT Core roles \[IoT.5\] deben estar etiquetados](#)
- [AWS IoT Core Las políticas \[IoT.6\] deben estar etiquetadas](#)
- [\[IoT Events .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoT Events .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Events .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Site Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Site Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)

- [\[IoT Twin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Twin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoT Wireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [\[RDS.1\] La instantánea de RDS debe ser privada](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[RedshiftServerless.3\] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público](#)
- [\[RedshiftServerless.4\] Los espacios de nombres de Redshift Serverless deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado](#)
- [\[RedshiftServerless.6\] Los espacios de nombres de Redshift Serverless deberían exportar los registros a los registros CloudWatch](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de base de datos predeterminado](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)

- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

Asia-Pacífico (Hong Kong)

Los siguientes controles no se admiten en la región de Asia Pacífico (Hong Kong).

- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)

- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Cognito.1\] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.24\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[IoTEvents.1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)

- [\[Io TEvents .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[Io TEvents .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[Io TSite Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[Io TSite Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[Io TSite Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[Io TSite Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[Io TSite Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[Io TTwin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[Io TWireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)

- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

Asia-Pacífico (Hyderabad)

Los siguientes controles no se admiten en la región de Asia Pacífico (Hyderabad).

- [\[Account.2\] Cuentas de AWS debe formar parte de una organización AWS Organizations](#)
- [\[APIGateway.8\] Las rutas de API Gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas V2 de API Gateway](#)
- [\[Amplify.1\] Las aplicaciones de Amplify deben estar etiquetadas](#)
- [\[Amplify.2\] Las ramas de Amplify deben estar etiquetadas](#)
- [\[AppConfig.1\] AWS AppConfig las aplicaciones deben estar etiquetadas](#)
- [\[AppConfig.2\] los perfiles de AWS AppConfig configuración deben estar etiquetados](#)
- [\[AppConfig.3\] AWS AppConfig los entornos deben estar etiquetados](#)
- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[Backup.1\] Los puntos AWS Backup de recuperación deben cifrarse en reposo](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)

- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CloudTrail.6\] Asegurar que los CloudTrail registros del bucket de S3 no son de acceso público](#)
- [\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el bucket de CloudTrail S3](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Cognito.1\] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.2\] Los certificados DMS deben estar etiquetados](#)
- [\[DMS.3\] Las suscripciones a eventos de DMS deben estar etiquetadas](#)
- [\[DMS.4\] Las instancias de replicación de DMS deben etiquetarse](#)
- [\[DMS.5\] Los grupos de subredes de replicación del DMS deben estar etiquetados](#)
- [\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)

- [\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)
- [\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado](#)
- [\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.14\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0.0.0/0 o: :/0 al puerto 3389](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)
- [\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.25\] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red](#)
- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad](#)
- [\[EC2.34\] Las tablas de enrutamiento de las puertas de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.40\] Las puertas de enlace de EC2 NAT deben etiquetarse](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben etiquetarse](#)
- [\[EC251\] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.170\] Las plantillas de EC2 lanzamiento deben usar el servicio de metadatos de instancias versión 2 \(\) IMDSv2](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.175\] Las plantillas de EC2 lanzamiento deben estar etiquetadas](#)

- [\[EC2.177\] las sesiones espejo EC2 de tráfico deberían estar etiquetadas](#)
- [\[EC2.179\] Los objetivos EC2 de tráfico reflejados deben estar etiquetados](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] Los volúmenes de Amazon EFS deben estar en los planes de respaldo](#)
- [\[ELB.14\] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.17\] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)
- [\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)
- [\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)
- [\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)
- [\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)
- [\[ES.4\] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[Glue.4\] Los trabajos de AWS Glue Spark deberían ejecutarse en versiones compatibles de AWS Glue](#)

- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)
- [\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)
- [\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)
- [\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)
- [\[IAM.19\] MFA se debe habilitar para todos los usuarios de IAM](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)
- [\[IAM.22\] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días](#)
- [\[IAM.24\] Los roles de IAM deben etiquetarse](#)
- [\[IAM.25\] Los usuarios de IAM deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IAM.27\] Las identidades de IAM no deben tener adjunta la política AWSCloud ShellFullAccess](#)
- [\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.2\] El análisis de ECR en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.4\] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado](#)
- [Los perfiles de AWS IoT Device Defender seguridad \[IoT.1\] deben estar etiquetados](#)
- [\[IoT.2\] las acciones de AWS IoT Core mitigación deben estar etiquetadas](#)
- [AWS IoT Core Las dimensiones de \[IoT.3\] deben estar etiquetadas](#)
- [Los AWS IoT Core autorizadores \[IoT.4\] deben estar etiquetados](#)
- [Los alias de los AWS IoT Core roles \[IoT.5\] deben estar etiquetados](#)
- [AWS IoT Core Las políticas \[IoT.6\] deben estar etiquetadas](#)
- [\[IoT Events .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoT Events .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)

- [\[Io TEvents .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[Io TSite Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[Io TSite Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[Io TSite Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[Io TSite Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[Io TSite Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[Io TTwin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[Io TWireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)
- [\[KMS.1\] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.2\] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)
- [\[MQ.2\] Los corredores de ActiveMQ deberían transmitir los registros de auditoría a CloudWatch](#)
- [\[MQ.3\] Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[MQ.4\] Los agentes de Amazon MQ deben estar etiquetados](#)
- [\[MQ.5\] Los corredores ActiveMQ deben usar el modo de implementación activo/en espera](#)
- [\[MQ.6\] Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)

- [\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [\[Neptune.4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación](#)
- [\[Neptune.5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas](#)
- [\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM](#)
- [\[Neptune.8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas](#)
- [\[Neptune.9\] Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad](#)
- [Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)
- [Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)
- [Los OpenSearch dominios \[Opensearch.3\] deben cifrar los datos enviados entre nodos](#)
- [El registro de errores de OpenSearch dominio \[Opensearch.4\] en CloudWatch Logs debe estar activado](#)
- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)
- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los OpenSearch dominios \[Opensearch.7\] deben tener habilitado un control de acceso detallado](#)
- [\[Opensearch.8\] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente](#)
- [Los OpenSearch dominios \[Opensearch.9\] deben estar etiquetados](#)
- [Los OpenSearch dominios \[Opensearch.10\] deben tener instalada la última actualización de software](#)
- [Los OpenSearch dominios \[Opensearch.11\] deben tener al menos tres nodos principales dedicados](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)

- [Los clústeres de bases de datos de RDS \[RDS.15\] deben configurarse para varias zonas de disponibilidad](#)
- [Las instancias de base de datos de RDS \[RDS.26\] deben protegerse mediante un plan de copias de seguridad](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[RDS.37\] Los clústeres de bases de datos Aurora PostgreSQL deberían publicar registros en Logs CloudWatch](#)
- [Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[RedshiftServerless.3\] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público](#)
- [\[RedshiftServerless.4\] Los espacios de nombres de Redshift Serverless deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado](#)
- [\[RedshiftServerless.6\] Los espacios de nombres de Redshift Serverless deberían exportar los registros a los registros CloudWatch](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de base de datos predeterminado](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.6\] Las políticas de compartimentos de uso general de S3 deberían restringir el acceso a otros Cuentas de AWS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] las instancias de SageMaker notebook deben lanzarse en una VPC personalizada](#)

- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook](#)
- [\[SageMaker.5\] SageMaker los modelos deberían bloquear el tráfico entrante](#)
- [\[SageMaker.6\] Las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas](#)
- [\[SageMaker.7\] SageMaker las imágenes deben estar etiquetadas](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SQS.3\] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público](#)
- [\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [\[Transfer.3\] Los conectores Transfer Family deben tener habilitado el registro](#)
- [\[Transfer.4\] Los acuerdos Transfer Family deben estar etiquetados](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [La AWS WAF web de \[WAF.10\] ACLs debe tener al menos una regla o grupo de reglas](#)
- [El registro de ACL AWS WAF web de \[WAF.11\] debe estar habilitado](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

Asia-Pacífico (Yakarta)

Los siguientes controles no se admiten en la región de Asia Pacífico (Yakarta).

- [\[Account.2\] Cuentas de AWS debe formar parte de una organización AWS Organizations](#)
- [\[APIGateway.8\] Las rutas de API Gateway deben especificar un tipo de autorización](#)

- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas V2 de API Gateway](#)
- [\[Amplify.1\] Las aplicaciones de Amplify deben estar etiquetadas](#)
- [\[Amplify.2\] Las ramas de Amplify deben estar etiquetadas](#)
- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[Backup.1\] Los puntos AWS Backup de recuperación deben cifrarse en reposo](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeBuild.1\] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales](#)
- [\[CodeBuild.2\] Las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro](#)

- [\[CodeBuild.3\] Los registros de CodeBuild S3 deben estar cifrados](#)
- [\[CodeBuild.4\] Los entornos de los CodeBuild proyectos deben tener una duración de registro AWS Config](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Cognito.1\] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.2\] Los certificados DMS deben estar etiquetados](#)
- [\[DMS.3\] Las suscripciones a eventos de DMS deben estar etiquetadas](#)
- [\[DMS.4\] Las instancias de replicación de DMS deben etiquetarse](#)
- [\[DMS.5\] Los grupos de subredes de replicación del DMS deben estar etiquetados](#)
- [\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)
- [\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado](#)
- [\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)

- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DocumentDb.6\] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.14\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 o: :/0 al puerto 3389](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)
- [\[EC2.24\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad](#)
- [\[EC2.51\] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.177\] las sesiones espejo EC2 de tráfico deberían estar etiquetadas](#)
- [\[EC2.179\] Los objetivos EC2 de tráfico reflejados deben estar etiquetados](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] Los volúmenes de Amazon EFS deben estar en los planes de respaldo](#)
- [\[ELB.17\] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas](#)

- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)
- [\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)
- [\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)
- [\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [Los perfiles de AWS IoT Device Defender seguridad \[IoT.1\] deben estar etiquetados](#)
- [\[IoT.2\] las acciones de AWS IoT Core mitigación deben estar etiquetadas](#)
- [AWS IoT Core Las dimensiones de \[IoT.3\] deben estar etiquetadas](#)
- [Los AWS IoT Core autorizadores \[IoT.4\] deben estar etiquetados](#)
- [Los alias de los AWS IoT Core roles \[IoT.5\] deben estar etiquetados](#)
- [AWS IoT Core Las políticas \[IoT.6\] deben estar etiquetadas](#)
- [\[IoT Events .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoT Events .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Events .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Site Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)

- [\[Io TSite Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[Io TSite Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[Io TSite Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[Io TSite Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[Io TTwin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[Io TWireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [\[Neptune.4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación](#)
- [\[Neptune.5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas](#)
- [\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM](#)
- [\[Neptune.8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas](#)

- [\[Neptune.9\] Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad](#)
- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)
- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [Las instancias de base de datos de RDS \[RDS.26\] deben protegerse mediante un plan de copias de seguridad](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.11\] Los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[ServiceCatalog.1\] Las carteras de Service Catalog solo deben compartirse dentro de una AWS organización](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SQS.3\] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público](#)
- [\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [La AWS WAF web de \[WAF.10\] ACLs debe tener al menos una regla o grupo de reglas](#)

- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

Asia-Pacífico (Malasia)

Los siguientes controles no se admiten en la región Asia Pacífico (Malasia).

- [\[ACM.1\] Los certificados importados y emitidos por ACM deben renovarse después de un período de tiempo específico](#)
- [\[ACM.2\] Los certificados RSA administrados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)
- [\[Cuenta.1\] La información de contacto de seguridad debe proporcionarse para un Cuenta de AWS](#)
- [\[Account.2\] Cuentas de AWS debe formar parte de una organización AWS Organizations](#)
- [\[APIGateway.8\] Las rutas de API Gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas V2 de API Gateway](#)
- [\[Amplify.1\] Las aplicaciones de Amplify deben estar etiquetadas](#)
- [\[Amplify.2\] Las ramas de Amplify deben estar etiquetadas](#)
- [\[AppConfig.1\] AWS AppConfig las aplicaciones deben estar etiquetadas](#)
- [\[AppConfig.2\] los perfiles de AWS AppConfig configuración deben estar etiquetados](#)
- [\[AppConfig.3\] AWS AppConfig los entornos deben estar etiquetados](#)
- [\[AppConfig.4\] Las asociaciones AWS AppConfig de extensiones deben estar etiquetadas](#)
- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.2\] AWS AppSync debe tener habilitado el registro a nivel de campo](#)
- [\[AppSync.4\] AWS AppSync APIs GraphQL debe estar etiquetado](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves de API](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[Athena.2\] Los catálogos de datos de Athena deben estar etiquetados](#)
- [\[Athena.3\] Los grupos de trabajo de Athena deben estar etiquetados](#)

- [\[Athena.4\] Los grupos de trabajo de Athena deben tener el registro habilitado](#)
- [\[AutoScaling.2\] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad](#)
- [\[AutoScaling.3\] Las configuraciones de lanzamiento de grupos de Auto Scaling deberían configurar las EC2 instancias para que requieran la versión 2 del Servicio de Metadatos de Instancia \(IMDSv2\)](#)
- [\[AutoScaling.6\] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad](#)
- [\[AutoScaling.9\] Los grupos de Amazon EC2 Auto Scaling deberían usar las plantillas de EC2 lanzamiento de Amazon](#)
- [\[Backup.1\] Los puntos AWS Backup de recuperación deben cifrarse en reposo](#)
- [\[Backup.2\] Los puntos AWS Backup de recuperación deben estar etiquetados](#)
- [\[Backup.3\] las AWS Backup bóvedas deben estar etiquetadas](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[Backup.5\] los planes de AWS Backup respaldo deben estar etiquetados](#)
- [\[Batch.1\] Las colas de trabajos por lotes deben estar etiquetadas](#)
- [\[Batch.2\] Las políticas de programación de lotes deben estar etiquetadas](#)
- [\[Batch.3\] Los entornos de procesamiento por lotes deben etiquetarse](#)
- [\[Batch.4\] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben etiquetarse](#)
- [\[CloudFormation.2\] las CloudFormation pilas deben estar etiquetadas](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)

- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CloudTrail.6\] Asegurar que los CloudTrail registros del bucket de S3 no son de acceso público](#)
- [\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el bucket de CloudTrail S3](#)
- [\[CloudTrail.10\] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [\[CloudWatch.17\] las acciones CloudWatch de alarma deben estar activadas](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeBuild.1\] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales](#)
- [\[CodeBuild.2\] Las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro](#)
- [\[CodeBuild.3\] Los registros de CodeBuild S3 deben estar cifrados](#)
- [\[CodeBuild.4\] Los entornos de los CodeBuild proyectos deben tener una duración de registro AWS Config](#)
- [\[CodeBuild.7\] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Cognito.1\] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[DataFirehose.1\] Los flujos de entrega de Firehose deben cifrarse en reposo](#)
- [\[DataSync.1\] DataSync las tareas deberían tener el registro activado](#)
- [\[DataSync.2\] DataSync las tareas deben estar etiquetadas](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.2\] Los certificados DMS deben estar etiquetados](#)

- [\[DMS.3\] Las suscripciones a eventos de DMS deben estar etiquetadas](#)
- [\[DMS.4\] Las instancias de replicación de DMS deben etiquetarse](#)
- [\[DMS.5\] Los grupos de subredes de replicación del DMS deben estar etiquetados](#)
- [\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)
- [\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado](#)
- [\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DocumentDb.6\] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.6\] Las tablas de DynamoDB deben tener la protección contra eliminación habilitada](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC24\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.21\] La red no ACLs debe permitir la entrada desde 0.0.0/0 al puerto 22 o al puerto 3389](#)

- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC2.24\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.25\] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red](#)
- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad](#)
- [\[EC2.33\] Las conexiones de puerta de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.34\] Las tablas de enrutamiento de las puertas de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.40\] Las puertas de enlace de EC2 NAT deben etiquetarse](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben etiquetarse](#)
- [\[EC2.51\] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)
- [\[EC2.52\] Las EC2 puertas de enlace de](#)
- [\[EC2.53\] Los grupos EC2 de seguridad no deberían permitir la entrada de 0.0.0.0/0 a los puertos de administración de servidores remotos](#)
- [\[EC2.54\] Los grupos EC2 de seguridad no deberían permitir la entrada de: :/0 a los puertos de administración de servidores remotos](#)
- [\[EC2.55\] VPCs debe configurarse con un punto final de interfaz para la API ECR](#)
- [\[EC2.56\] VPCs debe configurarse con un punto final de interfaz para Docker Registry](#)
- [\[EC2.57\] VPCs debe configurarse con un punto final de interfaz para Systems Manager](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.170\] Las plantillas de EC2 lanzamiento deben usar el servicio de metadatos de instancias versión 2 \(\) IMDSv2](#)
- [\[EC2.171\] Las conexiones EC2 VPN deben tener el registro habilitado](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.174\] Los conjuntos de opciones de EC2 DHCP deben estar etiquetados](#)
- [\[EC2.175\] Las plantillas de EC2 lanzamiento deben estar etiquetadas](#)

- [\[EC2.176\] Las listas de EC2 prefijos deben estar etiquetadas](#)
- [\[EC2.177\] las sesiones espejo EC2 de tráfico deberían estar etiquetadas](#)
- [\[EC2.178\] Los filtros espejo de EC2 tráfico deben estar etiquetados](#)
- [\[EC2.179\] Los objetivos EC2 de tráfico reflejados deben estar etiquetados](#)
- [\[ECR.1\] Los repositorios privados del ECR deben tener configurado el escaneo de imágenes](#)
- [\[ECR.2\] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas](#)
- [\[ECR.3\] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[ECR.5\] Los repositorios de ECR deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [\[ECS.3\] Las definiciones de tareas de ECS no deben compartir el espacio de nombres de los procesos del anfitrión](#)
- [\[ECS.4\] Los contenedores de ECS deben ejecutarse sin privilegios](#)
- [\[ECS.5\] Los contenedores ECS deben limitarse al acceso de solo lectura a los sistemas de archivos raíz](#)
- [\[ECS.8\] Los secretos no deben pasarse como variables de entorno del contenedor](#)
- [\[ECS.9\] Las definiciones de tareas de ECS deben tener una configuración de registro](#)
- [\[ECS.10\] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate](#)
- [\[ECS.12\] Los clústeres de ECS deben usar Container Insights](#)
- [\[ECS.16\] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas](#)
- [\[ECS.17\] Las definiciones de tareas de ECS no deben utilizar el modo de red host](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] Los volúmenes de Amazon EFS deben estar en los planes de respaldo](#)
- [\[EFS.3\] Los puntos de acceso EFS deben aplicar un directorio raíz](#)
- [\[EFS.4\] Los puntos de acceso EFS deben imponer una identidad de usuario](#)
- [\[EFS.5\] Los puntos de acceso de EFS deben etiquetarse](#)
- [\[EFS.6\] Los destinos de montaje de EFS no deben estar asociados a una subred pública](#)
- [\[EFS.7\] Los sistemas de archivos de EFS deben tener habilitadas las copias de seguridad automáticas](#)

- [\[EFS.8\] Los sistemas de archivos de EFS deben cifrarse en reposo](#)
- [\[EKS.2\] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible](#)
- [\[EKS.3\] Los clústeres de EKS deben usar secretos de Kubernetes cifrados](#)
- [\[EKS.6\] Los clústeres de EKS deben etiquetarse](#)
- [\[EKS.7\] Las configuraciones de los proveedores de identidad de EKS deben etiquetarse](#)
- [\[EKS.8\] Los clústeres de EKS deben tener habilitado el registro de auditoría](#)
- [\[ELB.10\] Equilibrador de carga clásico debe abarcar varias zonas de disponibilidad](#)
- [\[ELB.12\] Equilibrador de carga de aplicación debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.13\] Los equilibradores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad](#)
- [\[ELB.14\] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.17\] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.2\] ElastiCache Los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias](#)
- [\[ElastiCache.3\] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática](#)
- [\[ElastiCache.4\] los grupos de ElastiCache replicación deben estar cifrados en reposo](#)
- [\[ElastiCache.5\] los grupos de ElastiCache replicación deben cifrarse en tránsito](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)
- [\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)
- [\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)
- [\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)
- [\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)

- [\[EMR.2\] La configuración de bloqueo del acceso público de Amazon EMR debe estar habilitada](#)
- [\[EMR.3\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo](#)
- [\[EMR.4\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito](#)
- [\[ES.4\] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros](#)
- [\[ES.9\] Los dominios de Elasticsearch deben estar etiquetados](#)
- [\[EventBridge.2\] los autobuses de EventBridge eventos deben estar etiquetados](#)
- [\[EventBridge.3\] Los autobuses de eventos EventBridge personalizados deben incluir una política basada en los recursos](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FSx.1\] en el caso FSx de OpenZFS, los sistemas de archivos deben configurarse para copiar etiquetas en copias de seguridad y volúmenes](#)
- [\[FSx.2\] FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad](#)
- [\[FSx.3\] FSx para los sistemas de archivos OpenZFS, debe configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[FSx.4\] FSx para los sistemas de archivos NetApp ONTAP, debe configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[FSx.5\] FSx para Windows, los sistemas de archivos del servidor de archivos deben configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[Glue.1\] los AWS Glue trabajos deben estar etiquetados](#)
- [\[Glue.3\] Las transformaciones AWS Glue de aprendizaje automático deben cifrarse en reposo](#)
- [\[Glue.4\] Los trabajos de AWS Glue Spark deberían ejecutarse en versiones compatibles de AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)

- [\[GuardDuty.3\] GuardDuty IPSets debe estar etiquetado](#)
- [\[GuardDuty.4\] GuardDuty los detectores deben estar etiquetados](#)
- [\[GuardDuty.5\] La supervisión de registros de auditoría de GuardDuty EKS debe estar habilitada](#)
- [\[GuardDuty.6\] La protección de GuardDuty Lambda debe estar habilitada](#)
- [\[GuardDuty.7\] La supervisión en tiempo de ejecución de GuardDuty EKS debe estar habilitada](#)
- [\[GuardDuty.8\] La protección contra GuardDuty malware para EC2 debe estar habilitada](#)
- [\[GuardDuty.9\] La protección de GuardDuty RDS debe estar habilitada](#)
- [\[GuardDuty.10\] La protección de GuardDuty S3 debe estar habilitada](#)
- [\[GuardDuty.11\] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada](#)
- [\[GuardDuty.12\] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada](#)
- [\[GuardDuty.13\] La monitorización del GuardDuty EC2 tiempo de ejecución debe estar habilitada](#)
- [\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)
- [\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)
- [\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)
- [\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)
- [\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)
- [\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)
- [\[IAM.7\] Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)
- [\[IAM.10\] Las políticas de contraseñas de usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.11\] Asegurar que la política de contraseñas de IAM requiera al menos una letra mayúscula](#)
- [\[IAM.12\] Asegurar que la política de contraseñas de IAM requiera al menos una letra minúscula](#)
- [\[IAM.13\] Asegurar que la política de contraseñas de IAM requiera al menos un símbolo](#)
- [\[IAM.14\] Asegurar que la política de contraseñas de IAM requiera al menos un número](#)
- [\[IAM.15\] Asegurar que la política de contraseñas de IAM requiera una longitud mínima de 14 o más](#)
- [\[IAM.16\] Asegurar que la política de contraseñas de IAM impida la reutilización de contraseñas](#)

- [\[IAM.17\] Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos](#)
- [\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)
- [\[IAM.19\] MFA se debe habilitar para todos los usuarios de IAM](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)
- [\[IAM.22\] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días](#)
- [\[IAM.23\] Los analizadores del Analizador de acceso de IAM deben etiquetarse](#)
- [\[IAM.24\] Los roles de IAM deben etiquetarse](#)
- [\[IAM.25\] Los usuarios de IAM deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IAM.27\] Las identidades de IAM no deben tener adjunta la política AWSCloud ShellFullAccess](#)
- [\[IAM.28\] El analizador de acceso externo del Analizador de acceso de IAM debe habilitarse](#)
- [\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.2\] El análisis de ECR en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.4\] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado](#)
- [Los perfiles de AWS IoT Device Defender seguridad \[IoT.1\] deben estar etiquetados](#)
- [\[IoT.2\] las acciones de AWS IoT Core mitigación deben estar etiquetadas](#)
- [AWS IoT Core Las dimensiones de \[IoT.3\] deben estar etiquetadas](#)
- [Los AWS IoT Core autorizadores \[IoT.4\] deben estar etiquetados](#)
- [Los alias de los AWS IoT Core roles \[IoT.5\] deben estar etiquetados](#)
- [AWS IoT Core Las políticas \[IoT.6\] deben estar etiquetadas](#)
- [\[IoT Events .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoT Events .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Events .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Site Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)

- [\[Io TSite Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[Io TSite Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[Io TTwin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[Io TWireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)
- [\[Kinesis.1\] Las transmisiones de Kinesis deben cifrarse en reposo](#)
- [\[Kinesis.2\] Las transmisiones de Kinesis deben etiquetarse](#)
- [\[Kinesis.3\] Las transmisiones de Kinesis deben tener un periodo adecuado de retención de datos](#)
- [\[KMS.1\] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.2\] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.5\] Las claves KMS no deben ser de acceso público](#)
- [\[Lambda.5\] Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)
- [\[MQ.2\] Los corredores de ActiveMQ deberían transmitir los registros de auditoría a CloudWatch](#)
- [\[MQ.3\] Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[MQ.4\] Los agentes de Amazon MQ deben estar etiquetados](#)
- [\[MQ.5\] Los corredores ActiveMQ deben usar el modo de implementación activo/en espera](#)
- [\[MQ.6\] Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres](#)

- [\[MSK.1\] Los clústeres de MSK deben cifrarse en tránsito entre los nodos intermediarios](#)
- [\[MSK.2\] Los clústeres de MSK deberían tener configurada una supervisión mejorada](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [\[Neptune.4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación](#)
- [\[Neptune.5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas](#)
- [\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM](#)
- [\[Neptune.8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas](#)
- [\[Neptune.9\] Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad](#)
- [Los NetworkFirewall firewalls de Network Firewall se deben implementar en varias zonas de disponibilidad](#)
- [\[NetworkFirewall.2\] El registro de Network Firewall debe estar habilitado](#)
- [\[NetworkFirewall.3\] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas](#)
- [\[NetworkFirewall.4\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos](#)
- [\[NetworkFirewall.5\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados](#)
- [El grupo de reglas de Stateless Network Firewall \[NetworkFirewall.6\] no debe estar vacío](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de eliminación](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de cambio de subred](#)

- [Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)
- [Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)
- [Los OpenSearch dominios \[Opensearch.3\] deben cifrar los datos enviados entre nodos](#)
- [El registro de errores de OpenSearch dominio \[Opensearch.4\] en CloudWatch Logs debe estar activado](#)
- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)
- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los OpenSearch dominios \[Opensearch.7\] deben tener habilitado un control de acceso detallado](#)
- [\[Opensearch.8\] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente](#)
- [Los OpenSearch dominios \[Opensearch.9\] deben estar etiquetados](#)
- [Los OpenSearch dominios \[Opensearch.10\] deben tener instalada la última actualización de software](#)
- [Los OpenSearch dominios \[Opensearch.11\] deben tener al menos tres nodos principales dedicados](#)
- [La autoridad emisora de certificados AWS Private CA raíz \[PCA.1\] debe estar deshabilitada](#)
- [\[PCA.2\] Se debe etiquetar a las autoridades certificadoras de CA AWS privadas](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [Las instancias de RDS \[RDS.18\] deben implementarse en una VPC](#)
- [Los clústeres de bases de datos de RDS \[RDS.24\] deben usar un nombre de usuario de administrador personalizado](#)
- [Las instancias de bases de datos de RDS \[RDS.25\] deben usar un nombre de usuario de administrador personalizado](#)
- [Las instancias de base de datos de RDS \[RDS.26\] deben protegerse mediante un plan de copias de seguridad](#)
- [Los clústeres de bases de datos de RDS \[RDS.27\] deben cifrarse en reposo](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.34\] Los clústeres de bases de datos Aurora MySQL deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)

- [\[RDS.36\] Las instancias de base de datos de RDS para PostgreSQL deben publicar registros en Logs CloudWatch](#)
- [\[RDS.37\] Los clústeres de bases de datos Aurora PostgreSQL deberían publicar registros en Logs CloudWatch](#)
- [\[RDS.38\] Las instancias de base de datos de RDS para PostgreSQL deben cifrarse en tránsito](#)
- [\[RDS.39\] Las instancias de base de datos de RDS para MySQL deben cifrarse en tránsito](#)
- [\[RDS.40\] Las instancias de base de datos de RDS para SQL Server deberían publicar los registros en Logs CloudWatch](#)
- [\[RDS.41\] Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito](#)
- [\[RDS.42\] Las instancias de base de datos de RDS para MariaDB deberían publicar registros en Logs CloudWatch](#)
- [\[RDS.44\] El RDS para las instancias de base de datos MariaDB debe cifrarse en tránsito](#)
- [\[Redshift.1\] Los clústeres de Amazon Redshift deberían prohibir el acceso público](#)
- [Las conexiones a los clústeres de Amazon Redshift \[Redshift.2\] deben cifrarse en tránsito](#)
- [Los clústeres de Amazon Redshift \[Redshift.3\] deben tener habilitadas las instantáneas automáticas](#)
- [Los clústeres de Amazon Redshift \[Redshift.4\] deben tener habilitado el registro de auditoría](#)
- [Amazon Redshift \[Redshift.6\] debería tener habilitadas las actualizaciones automáticas a las versiones principales](#)
- [Los clústeres de Redshift \[Redshift.7\] deberían utilizar un enrutamiento de VPC mejorado](#)
- [Los clústeres de Amazon Redshift \[Redshift.8\] no deben usar el nombre de usuario de administrador predeterminado](#)
- [Los clústeres de Redshift \[Redshift.9\] no deben usar el nombre de base de datos predeterminado](#)
- [Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo](#)
- [\[Redshift.11\] Los clústeres de Redshift deben etiquetarse](#)
- [\[Redshift.13\] Las instantáneas del clúster de Redshift deben etiquetarse](#)
- [\[Redshift.15\] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos](#)
- [\[Redshift.16\] Los grupos de subredes de clústeres de Redshift deben tener subredes de varias zonas de disponibilidad](#)
- [\[Redshift.17\] Los grupos de parámetros del clúster de Redshift deben estar etiquetados](#)

- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[RedshiftServerless.3\] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público](#)
- [\[RedshiftServerless.4\] Los espacios de nombres de Redshift Serverless deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado](#)
- [\[RedshiftServerless.6\] Los espacios de nombres de Redshift Serverless deberían exportar los registros a los registros CloudWatch](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de base de datos predeterminado](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.7\] Los buckets de uso general de S3 deben usar la replicación entre regiones](#)
- [\[S3.10\] Los buckets de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida](#)
- [\[S3.11\] Los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos](#)
- [\[S3.12\] no ACLs debe usarse para administrar el acceso de los usuarios a los depósitos de uso general de S3](#)
- [\[S3.13\] Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida](#)
- [\[S3.19\] Los puntos de acceso de S3 deben tener habilitada la configuración de Bloqueo de acceso público](#)
- [\[S3.20\] Los buckets de uso general de S3 deben tener habilitada la eliminación de MFA](#)
- [\[S3.22\] Los buckets de uso general de S3 deben registrar eventos de escritura a nivel de objeto](#)
- [\[S3.23\] Los buckets de uso general de S3 deben registrar eventos de lectura a nivel de objeto](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)

- [\[SageMaker.2\] las instancias de SageMaker notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook](#)
- [\[SageMaker.4\] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1](#)
- [\[SageMaker.5\] SageMaker los modelos deberían bloquear el tráfico entrante](#)
- [\[SageMaker.6\] Las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas](#)
- [\[SageMaker.7\] SageMaker las imágenes deben estar etiquetadas](#)
- [\[SageMaker.8\] las instancias de SageMaker notebook deberían ejecutarse en plataformas compatibles](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [\[ServiceCatalog.1\] Las carteras de Service Catalog solo deben compartirse dentro de una AWS organización](#)
- [\[SNS.4\] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SQS.3\] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público](#)
- [\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [\[SSM.4\] Los documentos SSM no deben ser públicos](#)
- [\[SSM.5\] Los documentos SSM deben estar etiquetados](#)
- [\[StepFunctions.1\] Las máquinas de estado de Step Functions deberían tener el registro activado](#)
- [\[StepFunctions.2\] Las actividades de Step Functions deben estar etiquetadas](#)
- [Los AWS Transfer Family flujos de trabajo de \[Transfer.1\] deben estar etiquetados](#)
- [\[Transfer.2\] Los servidores de Transfer Family no deben utilizar el protocolo FTP para la conexión del punto de conexión](#)
- [\[Transfer.3\] Los conectores Transfer Family deben tener habilitado el registro](#)
- [\[Transfer.4\] Los acuerdos Transfer Family deben estar etiquetados](#)
- [\[Transfer.5\] Los certificados de Transfer Family deben estar etiquetados](#)

- [\[Transfer.6\] Los conectores Transfer Family deben estar etiquetados](#)
- [\[Transfer.7\] Los perfiles de Transfer Family deben estar etiquetados](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas de \[WAF.2\] Regionales AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.4\] Regionales AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [La AWS WAF web de \[WAF.10\] ACLs debe tener al menos una regla o grupo de reglas](#)
- [AWS WAF Las reglas de \[WAF.12\] deben tener habilitadas las métricas CloudWatch](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

Asia-Pacífico (Melbourne)

Los siguientes controles no se admiten en la región Asia Pacífico (Melbourne).

- [\[APIGateway.8\] Las rutas de API Gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas V2 de API Gateway](#)
- [\[Amplify.1\] Las aplicaciones de Amplify deben estar etiquetadas](#)
- [\[Amplify.2\] Las ramas de Amplify deben estar etiquetadas](#)
- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.2\] AWS AppSync debe tener habilitado el registro a nivel de campo](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves de API](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)

- [\[Backup.1\] Los puntos AWS Backup de recuperación deben cifrarse en reposo](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[Batch.1\] Las colas de trabajos por lotes deben estar etiquetadas](#)
- [\[Batch.3\] Los entornos de procesamiento por lotes deben etiquetarse](#)
- [\[Batch.4\] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Cognito.1\] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)

- [\[DMS.2\] Los certificados DMS deben estar etiquetados](#)
- [\[DMS.3\] Las suscripciones a eventos de DMS deben estar etiquetadas](#)
- [\[DMS.4\] Las instancias de replicación de DMS deben etiquetarse](#)
- [\[DMS.5\] Los grupos de subredes de replicación del DMS deben estar etiquetados](#)
- [\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)
- [\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado](#)
- [\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DocumentDb.6\] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.1\] Las instantáneas de Amazon EBS no se deben poder restaurar públicamente](#)
- [\[EC24\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)

- [\[EC2.8\] EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancias IMDSv2](#)
- [\[EC2.14\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0.0.0/0 o: :/0 al puerto 3389](#)
- [\[EC2.18\] Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC2.24\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.25\] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red](#)
- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad](#)
- [\[EC2.34\] Las tablas de enrutamiento de las puertas de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.40\] Las puertas de enlace de EC2 NAT deben etiquetarse](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben etiquetarse](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.170\] Las plantillas de EC2 lanzamiento deben usar el servicio de metadatos de instancias versión 2 \(\) IMDSv2](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.175\] Las plantillas de EC2 lanzamiento deben estar etiquetadas](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] Los volúmenes de Amazon EFS deben estar en los planes de respaldo](#)
- [\[ELB.14\] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)

- [\[ELB.17\] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.2\] ElastiCache Los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias](#)
- [\[ElastiCache.3\] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática](#)
- [\[ElastiCache.4\] los grupos de ElastiCache replicación deben estar cifrados en reposo](#)
- [\[ElastiCache.5\] los grupos de ElastiCache replicación deben cifrarse en tránsito](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)
- [\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)
- [\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)
- [\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)
- [\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)
- [\[ES.4\] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FSx.1\] en el caso FSx de OpenZFS, los sistemas de archivos deben configurarse para copiar etiquetas en copias de seguridad y volúmenes](#)
- [\[FSx.3\] FSx para los sistemas de archivos OpenZFS, debe configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)

- [\[Glue.4\] Los trabajos de AWS Glue Spark deberían ejecutarse en versiones compatibles de AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)
- [\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)
- [\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)
- [\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)
- [\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.10\] Las políticas de contraseñas de usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.11\] Asegurar que la política de contraseñas de IAM requiera al menos una letra mayúscula](#)
- [\[IAM.12\] Asegurar que la política de contraseñas de IAM requiera al menos una letra minúscula](#)
- [\[IAM.13\] Asegurar que la política de contraseñas de IAM requiera al menos un símbolo](#)
- [\[IAM.14\] Asegurar que la política de contraseñas de IAM requiera al menos un número](#)
- [\[IAM.15\] Asegurar que la política de contraseñas de IAM requiera una longitud mínima de 14 o más](#)
- [\[IAM.16\] Asegurar que la política de contraseñas de IAM impida la reutilización de contraseñas](#)
- [\[IAM.17\] Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos](#)
- [\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)
- [\[IAM.19\] MFA se debe habilitar para todos los usuarios de IAM](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)
- [\[IAM.22\] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días](#)
- [\[IAM.24\] Los roles de IAM deben etiquetarse](#)
- [\[IAM.25\] Los usuarios de IAM deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IAM.27\] Las identidades de IAM no deben tener adjunta la política AWSCloud ShellFullAccess](#)

- [\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.2\] El análisis de ECR en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.4\] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado](#)
- [Los perfiles de AWS IoT Device Defender seguridad \[IoT.1\] deben estar etiquetados](#)
- [\[IoT.2\] las acciones de AWS IoT Core mitigación deben estar etiquetadas](#)
- [AWS IoT Core Las dimensiones de \[IoT.3\] deben estar etiquetadas](#)
- [Los AWS IoT Core autorizadores \[IoT.4\] deben estar etiquetados](#)
- [Los alias de los AWS IoT Core roles \[IoT.5\] deben estar etiquetados](#)
- [AWS IoT Core Las políticas \[IoT.6\] deben estar etiquetadas](#)
- [\[IoT Events .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoT Events .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Events .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Site Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Site Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Twin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoT Wireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)
- [\[Kinesis.1\] Las transmisiones de Kinesis deben cifrarse en reposo](#)

- [\[KMS.1\] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.2\] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)
- [\[MQ.6\] Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [\[Neptune.4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación](#)
- [\[Neptune.5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas](#)
- [\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM](#)
- [\[Neptune.8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas](#)
- [\[Neptune.9\] Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad](#)
- [Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)
- [Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)
- [Los OpenSearch dominios \[Opensearch.3\] deben cifrar los datos enviados entre nodos](#)
- [El registro de errores de OpenSearch dominio \[Opensearch.4\] en CloudWatch Logs debe estar activado](#)
- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)
- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los OpenSearch dominios \[Opensearch.7\] deben tener habilitado un control de acceso detallado](#)

- [\[Opensearch.8\] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente](#)
- [Los OpenSearch dominios \[Opensearch.9\] deben estar etiquetados](#)
- [Los OpenSearch dominios \[Opensearch.10\] deben tener instalada la última actualización de software](#)
- [Los OpenSearch dominios \[Opensearch.11\] deben tener al menos tres nodos principales dedicados](#)
- [\[RDS.1\] La instantánea de RDS debe ser privada](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [Los clústeres de bases de datos de RDS \[RDS.15\] deben configurarse para varias zonas de disponibilidad](#)
- [Las instancias de base de datos de RDS \[RDS.26\] deben protegerse mediante un plan de copias de seguridad](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[RDS.37\] Los clústeres de bases de datos Aurora PostgreSQL deberían publicar registros en Logs CloudWatch](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[RedshiftServerless.3\] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público](#)
- [\[RedshiftServerless.4\] Los espacios de nombres de Redshift Serverless deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado](#)
- [\[RedshiftServerless.6\] Los espacios de nombres de Redshift Serverless deberían exportar los registros a los registros CloudWatch](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de base de datos predeterminado](#)

- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] las instancias de SageMaker notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook](#)
- [\[SageMaker.5\] SageMaker los modelos deberían bloquear el tráfico entrante](#)
- [\[SageMaker.6\] Las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas](#)
- [\[SageMaker.7\] SageMaker las imágenes deben estar etiquetadas](#)
- [\[SageMaker.8\] las instancias de SageMaker notebook deberían ejecutarse en plataformas compatibles](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SQS.3\] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público](#)
- [\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [\[SSM.4\] Los documentos SSM no deben ser públicos](#)
- [\[StepFunctions.1\] Las máquinas de estado de Step Functions deberían tener el registro activado](#)
- [\[Transfer.3\] Los conectores Transfer Family deben tener habilitado el registro](#)
- [\[Transfer.4\] Los acuerdos Transfer Family deben estar etiquetados](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

- [El registro de ACL AWS WAF web de \[WAF.11\] debe estar habilitado](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

Asia-Pacífico (Bombay)

Los siguientes controles no se admiten en la región de Asia Pacífico (Bombay).

- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)

- [\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[IoT Twin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoT Wireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

Asia-Pacífico (Osaka)

Los siguientes controles no se admiten en la región de Asia Pacífico (Osaka).

- [\[ACM.1\] Los certificados importados y emitidos por ACM deben renovarse después de un período de tiempo específico](#)

- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[Backup.1\] Los puntos AWS Backup de recuperación deben cifrarse en reposo](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)

- [\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DocumentDb.6\] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC24\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.8\] EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancias IMDSv2](#)
- [\[EC2.14\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0.0.0/0 o :::0 al puerto 3389](#)
- [\[EC220\] Ambos túneles de VPN de una conexión de AWS Site-to-Site VPN deben estar activos](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.55\] VPCs debe configurarse con un punto final de interfaz para la API ECR](#)
- [\[EC2.56\] VPCs debe configurarse con un punto final de interfaz para Docker Registry](#)
- [\[EC2.57\] VPCs debe configurarse con un punto final de interfaz para Systems Manager](#)

- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[ELB.1\] El equilibrador de carga de aplicación debe configurarse para redirigir todas las solicitudes HTTP a HTTPS](#)
- [\[ELB.2\] Los equilibradores de carga clásicos con agentes de escucha SSL/HTTPS deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.3\] Los oyentes de Equilibrador de carga clásico deben configurarse con una terminación HTTPS o TLS](#)
- [\[ELB.4\] El equilibrador de carga de aplicación debe configurarse para eliminar los encabezados http no válidos](#)
- [\[ELB.6\] La protección contra la eliminación de un equilibrador de carga de aplicación, de puerta de enlace y de red debe estar habilitada](#)
- [\[ELB.8\] Los equilibradores de carga clásicos con agentes de escucha SSL deben usar una política de seguridad predefinida que tenga una duración sólida AWS Config](#)
- [\[ELB.16\] Los equilibradores de carga de aplicaciones deben estar asociados a una ACL web de AWS WAF](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)
- [\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)
- [\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)
- [\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)

- [\[GlobalAccelerator.1\]](#) Los aceleradores de Global Accelerator deben estar etiquetados
- [\[IAM.4\]](#) La clave de acceso del usuario raíz de IAM no debería existir
- [\[IAM.18\]](#) Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support
- [\[IAM.26\]](#) Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse
- [\[Inspector.3\]](#) El análisis de código de Lambda en Amazon Inspector debe estar habilitado
- [Los perfiles de AWS IoT Device Defender seguridad \[IoT.1\]](#) deben estar etiquetados
- [\[IoT.2\]](#) las acciones de AWS IoT Core mitigación deben estar etiquetadas
- [AWS IoT Core Las dimensiones de \[IoT.3\]](#) deben estar etiquetadas
- [Los AWS IoT Core autorizadores \[IoT.4\]](#) deben estar etiquetados
- [Los alias de los AWS IoT Core roles \[IoT.5\]](#) deben estar etiquetados
- [AWS IoT Core Las políticas \[IoT.6\]](#) deben estar etiquetadas
- [\[IoT Events .1\]](#) Las entradas de AWS IoT Events deben estar etiquetadas
- [\[IoT Events .2\]](#) Los modelos de detectores de AWS IoT Events deben estar etiquetados
- [\[IoT Events .3\]](#) Los modelos de alarma de AWS IoT Events deben estar etiquetados
- [\[IoT Site Wise.1\]](#) Los modelos de SiteWise activos de AWS IoT deben estar etiquetados
- [\[IoT Site Wise.2\]](#) SiteWise Los paneles de AWS IoT deben estar etiquetados
- [\[IoT Site Wise.3\]](#) SiteWise Las pasarelas de AWS IoT deben estar etiquetadas
- [\[IoT Site Wise.4\]](#) Los SiteWise portales de AWS IoT deben estar etiquetados
- [\[IoT Site Wise.5\]](#) Los SiteWise proyectos de AWS IoT deben estar etiquetados
- [\[IoT Twin Maker.1\]](#) Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados
- [\[IoT Twin Maker.2\]](#) Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados
- [\[IoT Twin Maker.3\]](#) TwinMaker Las escenas de AWS IoT deben estar etiquetadas
- [\[IoT Twin Maker.4\]](#) TwinMaker Las entidades de AWS IoT deben estar etiquetadas
- [\[IoT Wireless .1\]](#) Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados
- [\[IoT Wireless .2\]](#) Los perfiles del servicio AWS IoT Wireless deben estar etiquetados
- [\[IoT Wireless .3\]](#) Las tareas de AWS IoT FUOTA deben estar etiquetadas
- [\[IVS.1\]](#) Los pares de teclas de reproducción del IVS deben estar etiquetados
- [\[IVS.2\]](#) Las configuraciones de grabación del IVS deben estar etiquetadas
- [\[IVS.3\]](#) Los canales de IVS deben estar etiquetados
- [\[Keyspaces.1\]](#) Los espacios clave de Amazon Keyspaces deben estar etiquetados

- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[RedshiftServerless.3\] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público](#)
- [\[RedshiftServerless.4\] Los espacios de nombres de Redshift Serverless deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado](#)
- [\[RedshiftServerless.6\] Los espacios de nombres de Redshift Serverless deberían exportar los registros a los registros CloudWatch](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de base de datos predeterminado](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SSM.2\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de parche de COMPLIANT después de la instalación de un parche](#)
- [\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [La AWS WAF web de \[WAF.10\] ACLs debe tener al menos una regla o grupo de reglas](#)
- [El registro de ACL AWS WAF web de \[WAF.11\] debe estar habilitado](#)

- [\[WorkSpaces.1\]](#) los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [\[WorkSpaces.2\]](#) los volúmenes WorkSpaces raíz deben cifrarse en reposo

Asia-Pacífico (Seúl)

Los siguientes controles no se admiten en la región de Asia Pacífico (Seúl).

- [\[AppRunner.1\]](#) Los servicios de App Runner deben estar etiquetados
- [\[AppRunner.2\]](#) Los conectores VPC de App Runner deben estar etiquetados
- [\[AppSync.1\]](#) Las cachés de las AWS AppSync API deben cifrarse en reposo
- [\[AppSync.6\]](#) Las cachés de las AWS AppSync API deben cifrarse en tránsito
- [\[CloudFront.1\]](#) CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [\[CloudFront.3\]](#) CloudFront las distribuciones deben requerir el cifrado en tránsito
- [\[CloudFront.4\]](#) CloudFront Las distribuciones deben tener configurada la conmutación por error de origen
- [\[CloudFront.5\]](#) CloudFront las distribuciones deben tener el registro habilitado
- [\[CloudFront.6\]](#) CloudFront Las distribuciones deben tener WAF habilitado
- [\[CloudFront.7\]](#) CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados
- [\[CloudFront.8\]](#) CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS
- [\[CloudFront.9\]](#) CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados
- [\[CloudFront.10\]](#) CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados
- [\[CloudFront.12\]](#) CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes
- [\[CloudFront.13\]](#) CloudFront Las distribuciones deben usar el control de acceso de origen
- [\[CloudFront.14\]](#) CloudFront Las distribuciones deben etiquetarse
- [\[CodeArtifact.1\]](#) CodeArtifact Los repositorios deben estar etiquetados
- [\[CodeGuruProfiler.1\]](#) Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados
- [\[CodeGuruReviewer.1\]](#) Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [\[DynamoDB.3\]](#) Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo

- [\[DynamoDB.7\]](#) Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito
- [\[EC224\]](#) No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon
- [\[EC2.173\]](#) Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [\[ECR.4\]](#) Los repositorios públicos de ECR deben estar etiquetados
- [\[FraudDetector.1\]](#) Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [\[FraudDetector.2\]](#) Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [\[FraudDetector.3\]](#) Los resultados de Amazon Fraud Detector deben estar etiquetados
- [\[FraudDetector.4\]](#) Las variables de Amazon Fraud Detector deben estar etiquetadas
- [\[GlobalAccelerator.1\]](#) Los aceleradores de Global Accelerator deben estar etiquetados
- [\[Glue.4\]](#) Los trabajos de AWS Glue Spark deberían ejecutarse en versiones compatibles de AWS Glue
- [\[IAM.26\]](#) Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse
- [\[Inspector.3\]](#) El análisis de código de Lambda en Amazon Inspector debe estar habilitado
- [\[IoT Twin Maker.4\]](#) TwinMaker Las entidades de AWS IoT deben estar etiquetadas
- [\[IoT Wireless .1\]](#) Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados
- [\[IoT Wireless .2\]](#) Los perfiles del servicio AWS IoT Wireless deben estar etiquetados
- [\[IoT Wireless .3\]](#) Las tareas de AWS IoT FUOTA deben estar etiquetadas
- [\[RDS.31\]](#) Los grupos de seguridad de bases de datos de RDS deben etiquetarse
- [\[Route53.1\]](#) Las comprobaciones de estado de Route 53 deben estar etiquetadas
- [Las zonas alojadas públicas de Route 53 \[Route53.2\]](#) deben registrar las consultas de DNS
- [\[S3.24\]](#) Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\]](#) debe estar habilitado
- [Las reglas globales de \[WAF.6\]](#) AWS WAF clásicas deben tener al menos una condición
- [Los grupos de reglas globales de \[WAF.7\]](#) AWS WAF clásicos deben tener al menos una regla
- [La web de \[WAF.8\]](#) global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas

Asia-Pacífico (Singapur)

Los siguientes controles no se admiten en la región Asia Pacífico (Singapur).

- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IoTWireless.1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoTWireless.2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[IoTWireless.3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)

- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

Asia-Pacífico (Sídney)

Los siguientes controles no se admiten en la región de Asia Pacífico (Sídney).

- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)

- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

Asia-Pacífico (Tailandia)

Los siguientes controles no se admiten en la región Asia Pacífico (Tailandia).

- [\[ACM.1\] Los certificados importados y emitidos por ACM deben renovarse después de un período de tiempo específico](#)
- [\[ACM.2\] Los certificados RSA administrados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)
- [\[ACM.3\] Los certificados ACM deben estar etiquetados](#)
- [\[Cuenta.1\] La información de contacto de seguridad debe proporcionarse para un Cuenta de AWS](#)
- [\[Account.2\] Cuentas de AWS debe formar parte de una organización AWS Organizations](#)
- [\[APIGateway.1\] El registro de ejecución de WebSocket REST y API de API Gateway debe estar habilitado](#)
- [\[APIGateway.5\] Los datos de la caché de la API de REST de API Gateway deben cifrarse en reposo](#)
- [\[APIGateway.8\] Las rutas de API Gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas V2 de API Gateway](#)
- [\[Amplify.1\] Las aplicaciones de Amplify deben estar etiquetadas](#)
- [\[Amplify.2\] Las ramas de Amplify deben estar etiquetadas](#)

- [\[AppConfig.1\] AWS AppConfig las aplicaciones deben estar etiquetadas](#)
- [\[AppConfig.2\] los perfiles de AWS AppConfig configuración deben estar etiquetados](#)
- [\[AppConfig.3\] AWS AppConfig los entornos deben estar etiquetados](#)
- [\[AppConfig.4\] Las asociaciones AWS AppConfig de extensiones deben estar etiquetadas](#)
- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.2\] AWS AppSync debe tener habilitado el registro a nivel de campo](#)
- [\[AppSync.4\] AWS AppSync APIs GraphQL debe estar etiquetado](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves de API](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[Athena.2\] Los catálogos de datos de Athena deben estar etiquetados](#)
- [\[Athena.3\] Los grupos de trabajo de Athena deben estar etiquetados](#)
- [\[Athena.4\] Los grupos de trabajo de Athena deben tener el registro habilitado](#)
- [\[AutoScaling.2\] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad](#)
- [\[AutoScaling.3\] Las configuraciones de lanzamiento de grupos de Auto Scaling deberían configurar las EC2 instancias para que requieran la versión 2 del Servicio de Metadatos de Instancia \(IMDSv2\)](#)
- [\[AutoScaling.6\] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad](#)
- [\[AutoScaling.9\] Los grupos de Amazon EC2 Auto Scaling deberían usar las plantillas de EC2 lanzamiento de Amazon](#)
- [\[AutoScaling.10\] Los grupos EC2 de Auto Scaling deben estar etiquetados](#)
- [\[Backup.1\] Los puntos AWS Backup de recuperación deben cifrarse en reposo](#)
- [\[Backup.2\] Los puntos AWS Backup de recuperación deben estar etiquetados](#)
- [\[Backup.3\] las AWS Backup bóvedas deben estar etiquetadas](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[Backup.5\] los planes de AWS Backup respaldo deben estar etiquetados](#)
- [\[Batch.1\] Las colas de trabajos por lotes deben estar etiquetadas](#)
- [\[Batch.2\] Las políticas de programación de lotes deben estar etiquetadas](#)

- [\[Batch.3\] Los entornos de procesamiento por lotes deben etiquetarse](#)
- [\[Batch.4\] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben etiquetarse](#)
- [\[CloudFormation.2\] las CloudFormation pilas deben estar etiquetadas](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CloudTrail.6\] Asegurar que los CloudTrail registros del bucket de S3 no son de acceso público](#)
- [\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el bucket de CloudTrail S3](#)
- [\[CloudTrail.9\] los registros de CloudTrail seguimiento deben etiquetarse](#)
- [\[CloudTrail.10\] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [\[CloudWatch.17\] las acciones CloudWatch de alarma deben estar activadas](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeBuild.1\] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales](#)
- [\[CodeBuild.2\] Las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro](#)
- [\[CodeBuild.3\] Los registros de CodeBuild S3 deben estar cifrados](#)

- [\[CodeBuild.4\] Los entornos de los CodeBuild proyectos deben tener una duración de registro AWS Config](#)
- [\[CodeBuild.7\] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Cognito.1\] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[DataFirehose.1\] Los flujos de entrega de Firehose deben cifrarse en reposo](#)
- [\[DataSync.1\] DataSync las tareas deberían tener el registro activado](#)
- [\[DataSync.2\] DataSync las tareas deben estar etiquetadas](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)
- [\[DMS.2\] Los certificados DMS deben estar etiquetados](#)
- [\[DMS.3\] Las suscripciones a eventos de DMS deben estar etiquetadas](#)
- [\[DMS.4\] Las instancias de replicación de DMS deben etiquetarse](#)
- [\[DMS.5\] Los grupos de subredes de replicación del DMS deben estar etiquetados](#)
- [\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)
- [\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado](#)

- [\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DocumentDb.6\] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.5\] Las tablas de DynamoDB deben etiquetarse](#)
- [\[DynamoDB.6\] Las tablas de DynamoDB deben tener la protección contra eliminación habilitada](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC24\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.21\] La red no ACLs debe permitir la entrada desde 0.0.0/0 al puerto 22 o al puerto 3389](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.25\] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red](#)
- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad](#)
- [\[EC2.33\] Las conexiones de puerta de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.34\] Las tablas de enrutamiento de las puertas de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.35\] Las interfaces EC2 de red deben etiquetarse](#)
- [\[EC2.36\] Las pasarelas de EC2 clientes deben estar etiquetadas](#)
- [\[EC2.37\] Las direcciones IP EC2 elásticas deben etiquetarse](#)

- [\[EC2.38\] EC2 las instancias deben estar etiquetadas](#)
- [\[EC2.39\] Las puertas de enlace de EC2 Internet deben etiquetarse](#)
- [\[EC2.40\] Las puertas de enlace de EC2 NAT deben etiquetarse](#)
- [La EC2 red \[EC2.41\] ACLs debe estar etiquetada](#)
- [\[EC2.42\] Las tablas de EC2 enrutamiento deben estar etiquetadas](#)
- [\[EC2.43\] los grupos EC2 de seguridad deben estar etiquetados](#)
- [EC2 Las subredes \[EC2.44\] deben estar etiquetadas](#)
- [\[EC2.45\] los EC2 volúmenes deben estar etiquetados](#)
- [\[EC2.46\] Amazon VPCs debería estar etiquetado](#)
- [\[EC2.47\] Los servicios de puntos de conexión de Amazon VPC deben etiquetarse](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben etiquetarse](#)
- [\[EC2.49\] Las conexiones de emparejamiento de Amazon VPC deben etiquetarse](#)
- [\[EC2.50\] Las puertas de enlace de EC2 VPN deben etiquetarse](#)
- [\[EC251\] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)
- [\[EC2.52\] Las EC2 puertas de enlace de](#)
- [\[EC2.53\] Los grupos EC2 de seguridad no deberían permitir la entrada de 0.0.0.0/0 a los puertos de administración de servidores remotos](#)
- [\[EC2.54\] Los grupos EC2 de seguridad no deberían permitir la entrada de: :/0 a los puertos de administración de servidores remotos](#)
- [\[EC2.55\] VPCs debe configurarse con un punto final de interfaz para la API ECR](#)
- [\[EC2.56\] VPCs debe configurarse con un punto final de interfaz para Docker Registry](#)
- [\[EC2.57\] VPCs debe configurarse con un punto final de interfaz para Systems Manager](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.170\] Las plantillas de EC2 lanzamiento deben usar el servicio de metadatos de instancias versión 2 \(\) IMDSv2](#)
- [\[EC2.171\] Las conexiones EC2 VPN deben tener el registro habilitado](#)
- [\[EC2.172\] La configuración del acceso público al bloqueo de EC2 VPC debería bloquear el tráfico de las puertas de enlace de Internet](#)

- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.174\] Los conjuntos de opciones de EC2 DHCP deben estar etiquetados](#)
- [\[EC2.175\] Las plantillas de EC2 lanzamiento deben estar etiquetadas](#)
- [\[EC2.176\] Las listas de EC2 prefijos deben estar etiquetadas](#)
- [\[EC2.177\] las sesiones espejo EC2 de tráfico deberían estar etiquetadas](#)
- [\[EC2.178\] Los filtros espejo de EC2 tráfico deben estar etiquetados](#)
- [\[EC2.179\] Los objetivos EC2 de tráfico reflejados deben estar etiquetados](#)
- [\[ECR.1\] Los repositorios privados del ECR deben tener configurado el escaneo de imágenes](#)
- [\[ECR.2\] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas](#)
- [\[ECR.3\] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[ECR.5\] Los repositorios de ECR deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [\[ECS.2\] Los servicios de ECS no deberían tener direcciones IP públicas asignadas automáticamente](#)
- [\[ECS.3\] Las definiciones de tareas de ECS no deben compartir el espacio de nombres de los procesos del anfitrión](#)
- [\[ECS.4\] Los contenedores de ECS deben ejecutarse sin privilegios](#)
- [\[ECS.5\] Los contenedores ECS deben limitarse al acceso de solo lectura a los sistemas de archivos raíz](#)
- [\[ECS.8\] Los secretos no deben pasarse como variables de entorno del contenedor](#)
- [\[ECS.9\] Las definiciones de tareas de ECS deben tener una configuración de registro](#)
- [\[ECS.10\] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate](#)
- [\[ECS.12\] Los clústeres de ECS deben usar Container Insights](#)
- [\[ECS.13\] Los servicios de ECS deben estar etiquetados](#)
- [\[ECS.14\] Los clústeres de ECS deben etiquetarse](#)
- [\[ECS.15\] Las definiciones de tareas de ECS deben etiquetarse](#)
- [\[ECS.16\] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas](#)
- [\[ECS.17\] Las definiciones de tareas de ECS no deben utilizar el modo de red host](#)

- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] Los volúmenes de Amazon EFS deben estar en los planes de respaldo](#)
- [\[EFS.3\] Los puntos de acceso EFS deben aplicar un directorio raíz](#)
- [\[EFS.4\] Los puntos de acceso EFS deben imponer una identidad de usuario](#)
- [\[EFS.5\] Los puntos de acceso de EFS deben etiquetarse](#)
- [\[EFS.6\] Los destinos de montaje de EFS no deben estar asociados a una subred pública](#)
- [\[EFS.7\] Los sistemas de archivos de EFS deben tener habilitadas las copias de seguridad automáticas](#)
- [\[EFS.8\] Los sistemas de archivos de EFS deben cifrarse en reposo](#)
- [\[EKS.2\] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible](#)
- [\[EKS.3\] Los clústeres de EKS deben usar secretos de Kubernetes cifrados](#)
- [\[EKS.6\] Los clústeres de EKS deben etiquetarse](#)
- [\[EKS.7\] Las configuraciones de los proveedores de identidad de EKS deben etiquetarse](#)
- [\[EKS.8\] Los clústeres de EKS deben tener habilitado el registro de auditoría](#)
- [\[ELB.7\] Los equilibradores de carga clásicos deberían tener habilitado el drenaje de conexiones](#)
- [\[ELB.10\] Equilibrador de carga clásico debe abarcar varias zonas de disponibilidad](#)
- [\[ELB.12\] Equilibrador de carga de aplicación debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.13\] Los equilibradores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad](#)
- [\[ELB.14\] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.17\] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.2\] ElastiCache Los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias](#)
- [\[ElastiCache.3\] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática](#)
- [\[ElastiCache.4\] los grupos de ElastiCache replicación deben estar cifrados en reposo](#)

- [\[ElastiCache.5\] los grupos de ElastiCache replicación deben cifrarse en tránsito](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)
- [\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)
- [\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)
- [\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)
- [\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)
- [\[EMR.2\] La configuración de bloqueo del acceso público de Amazon EMR debe estar habilitada](#)
- [\[EMR.3\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo](#)
- [\[EMR.4\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito](#)
- [\[ES.3\] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos](#)
- [\[ES.4\] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros](#)
- [\[ES.5\] Los dominios de Elasticsearch deben tener habilitado el registro de auditoría](#)
- [\[ES.6\] Los dominios de Elasticsearch deben tener al menos tres nodos de datos](#)
- [\[ES.7\] Los dominios de Elasticsearch deben configurarse con al menos tres nodos maestros dedicados](#)
- [\[ES.8\] Las conexiones a dominios de Elasticsearch deben estar cifradas conforme a la política de seguridad TLS más reciente](#)
- [\[ES.9\] Los dominios de Elasticsearch deben estar etiquetados](#)
- [\[EventBridge.2\] los autobuses de EventBridge eventos deben estar etiquetados](#)
- [\[EventBridge.3\] Los autobuses de eventos EventBridge personalizados deben incluir una política basada en los recursos](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)

- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FSx.1\] en el caso FSx de OpenZFS, los sistemas de archivos deben configurarse para copiar etiquetas en copias de seguridad y volúmenes](#)
- [\[FSx.2\] FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad](#)
- [\[FSx.3\] FSx para los sistemas de archivos OpenZFS, debe configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[FSx.4\] FSx para los sistemas de archivos NetApp ONTAP, debe configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[FSx.5\] FSx para Windows, los sistemas de archivos del servidor de archivos deben configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[Glue.1\] los AWS Glue trabajos deben estar etiquetados](#)
- [\[Glue.3\] Las transformaciones AWS Glue de aprendizaje automático deben cifrarse en reposo](#)
- [\[Glue.4\] Los trabajos de AWS Glue Spark deberían ejecutarse en versiones compatibles de AWS Glue](#)
- [\[GuardDuty.1\] GuardDuty debería estar activado](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[GuardDuty.3\] GuardDuty IPSets debe estar etiquetado](#)
- [\[GuardDuty.4\] GuardDuty los detectores deben estar etiquetados](#)
- [\[GuardDuty.5\] La supervisión de registros de auditoría de GuardDuty EKS debe estar habilitada](#)
- [\[GuardDuty.6\] La protección de GuardDuty Lambda debe estar habilitada](#)
- [\[GuardDuty.7\] La supervisión en tiempo de ejecución de GuardDuty EKS debe estar habilitada](#)
- [\[GuardDuty.8\] La protección contra GuardDuty malware para EC2 debe estar habilitada](#)
- [\[GuardDuty.9\] La protección de GuardDuty RDS debe estar habilitada](#)
- [\[GuardDuty.10\] La protección de GuardDuty S3 debe estar habilitada](#)
- [\[GuardDuty.11\] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada](#)
- [\[GuardDuty.12\] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada](#)
- [\[GuardDuty.13\] La monitorización del GuardDuty EC2 tiempo de ejecución debe estar habilitada](#)
- [\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)

- [\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)
- [\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)
- [\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)
- [\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)
- [\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)
- [\[IAM.7\] Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)
- [\[IAM.10\] Las políticas de contraseñas de usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.11\] Asegurar que la política de contraseñas de IAM requiera al menos una letra mayúscula](#)
- [\[IAM.12\] Asegurar que la política de contraseñas de IAM requiera al menos una letra minúscula](#)
- [\[IAM.13\] Asegurar que la política de contraseñas de IAM requiera al menos un símbolo](#)
- [\[IAM.14\] Asegurar que la política de contraseñas de IAM requiera al menos un número](#)
- [\[IAM.15\] Asegurar que la política de contraseñas de IAM requiera una longitud mínima de 14 o más](#)
- [\[IAM.16\] Asegurar que la política de contraseñas de IAM impida la reutilización de contraseñas](#)
- [\[IAM.17\] Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos](#)
- [\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)
- [\[IAM.19\] MFA se debe habilitar para todos los usuarios de IAM](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)
- [\[IAM.22\] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días](#)
- [\[IAM.23\] Los analizadores del Analizador de acceso de IAM deben etiquetarse](#)
- [\[IAM.24\] Los roles de IAM deben etiquetarse](#)
- [\[IAM.25\] Los usuarios de IAM deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IAM.27\] Las identidades de IAM no deben tener adjunta la política AWSCloud ShellFullAccess](#)

- [\[IAM.28\] El analizador de acceso externo del Analizador de acceso de IAM debe habilitarse](#)
- [\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.2\] El análisis de ECR en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.4\] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado](#)
- [Los perfiles de AWS IoT Device Defender seguridad \[IoT.1\] deben estar etiquetados](#)
- [\[IoT.2\] las acciones de AWS IoT Core mitigación deben estar etiquetadas](#)
- [AWS IoT Core Las dimensiones de \[IoT.3\] deben estar etiquetadas](#)
- [Los AWS IoT Core autorizadores \[IoT.4\] deben estar etiquetados](#)
- [Los alias de los AWS IoT Core roles \[IoT.5\] deben estar etiquetados](#)
- [AWS IoT Core Las políticas \[IoT.6\] deben estar etiquetadas](#)
- [\[IoTEvents .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoTEvents .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoTEvents .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoTSiteWise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoTSiteWise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[IoT TwinMaker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoT TwinMaker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoT TwinMaker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoT TwinMaker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoTWireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoTWireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[IoTWireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)

- [\[Kinesis.1\] Las transmisiones de Kinesis deben cifrarse en reposo](#)
- [\[Kinesis.2\] Las transmisiones de Kinesis deben etiquetarse](#)
- [\[Kinesis.3\] Las transmisiones de Kinesis deben tener un periodo adecuado de retención de datos](#)
- [\[KMS.1\] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.2\] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.3\] no AWS KMS keys debe eliminarse involuntariamente](#)
- [\[KMS.5\] Las claves KMS no deben ser de acceso público](#)
- [\[Lambda.5\] Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad](#)
- [\[Lambda.6\] Las funciones de Lambda deben estar etiquetadas](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)
- [\[MQ.2\] Los corredores de ActiveMQ deberían transmitir los registros de auditoría a CloudWatch](#)
- [\[MQ.3\] Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[MQ.4\] Los agentes de Amazon MQ deben estar etiquetados](#)
- [\[MQ.5\] Los corredores ActiveMQ deben usar el modo de implementación activo/en espera](#)
- [\[MQ.6\] Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres](#)
- [\[MSK.1\] Los clústeres de MSK deben cifrarse en tránsito entre los nodos intermediarios](#)
- [\[MSK.2\] Los clústeres de MSK deberían tener configurada una supervisión mejorada](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [\[Neptune.4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación](#)
- [\[Neptune.5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas](#)
- [\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)

- [\[Neptune.7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM](#)
- [\[Neptune.8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas](#)
- [\[Neptune.9\] Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad](#)
- [Los NetworkFirewall firewalls de Network Firewall se deben implementar en varias zonas de disponibilidad](#)
- [\[NetworkFirewall.2\] El registro de Network Firewall debe estar habilitado](#)
- [\[NetworkFirewall.3\] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas](#)
- [\[NetworkFirewall.4\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos](#)
- [\[NetworkFirewall.5\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados](#)
- [El grupo de reglas de Stateless Network Firewall \[NetworkFirewall.6\] no debe estar vacío](#)
- [Los NetworkFirewall firewalls de Network Firewall se deben etiquetar](#)
- [\[NetworkFirewall.8\] Las políticas de firewall de Network Firewall se deben etiquetar](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de eliminación](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de cambio de subred](#)
- [Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)
- [Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)
- [Los OpenSearch dominios \[Opensearch.3\] deben cifrar los datos enviados entre nodos](#)
- [El registro de errores de OpenSearch dominio \[Opensearch.4\] en CloudWatch Logs debe estar activado](#)
- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)
- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los OpenSearch dominios \[Opensearch.7\] deben tener habilitado un control de acceso detallado](#)
- [\[Opensearch.8\] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente](#)

- [Los OpenSearch dominios \[Opensearch.9\] deben estar etiquetados](#)
- [Los OpenSearch dominios \[Opensearch.10\] deben tener instalada la última actualización de software](#)
- [Los OpenSearch dominios \[Opensearch.11\] deben tener al menos tres nodos principales dedicados](#)
- [La autoridad emisora de certificados AWS Private CA raíz \[PCA.1\] debe estar deshabilitada](#)
- [\[PCA.2\] Se debe etiquetar a las autoridades certificadoras de CA AWS privadas](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [Los clústeres de bases de datos de RDS \[RDS.16\] deben configurarse para copiar etiquetas en las instantáneas](#)
- [Las instancias de base de datos de RDS \[RDS.17\] deben configurarse para copiar etiquetas en las instantáneas](#)
- [Las instancias de RDS \[RDS.18\] deben implementarse en una VPC](#)
- [Las suscripciones de notificación de eventos de RDS \[RDS.19\] existentes deben configurarse para los eventos de clúster críticos](#)
- [Las suscripciones de notificación de eventos de RDS \[RDS.20\] existentes deben configurarse para eventos críticos de instancias de bases de datos](#)
- [Se debe configurar una suscripción a las notificaciones de eventos de RDS \[RDS.21\] para los eventos críticos de los grupos de parámetros de bases de datos](#)
- [Se debe configurar una suscripción a las notificaciones de eventos de RDS \[RDS.22\] para los eventos críticos de los grupos de seguridad de bases de datos](#)
- [Las instancias RDS \[RDS.23\] no deben usar el puerto predeterminado de un motor de base de datos](#)
- [Los clústeres de bases de datos de RDS \[RDS.24\] deben usar un nombre de usuario de administrador personalizado](#)
- [Las instancias de bases de datos de RDS \[RDS.25\] deben usar un nombre de usuario de administrador personalizado](#)
- [Las instancias de base de datos de RDS \[RDS.26\] deben protegerse mediante un plan de copias de seguridad](#)
- [Los clústeres de bases de datos de RDS \[RDS.27\] deben cifrarse en reposo](#)
- [\[RDS.28\] Los clústeres de base de datos de RDS deben etiquetarse](#)
- [\[RDS.29\] Las instantáneas del clúster de base de datos de RDS deben etiquetarse](#)

- [\[RDS.30\] Las instancias de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.32\] Las instantáneas de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.33\] Los grupos de subredes de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.34\] Los clústeres de bases de datos Aurora MySQL deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[RDS.36\] Las instancias de base de datos de RDS para PostgreSQL deben publicar registros en Logs CloudWatch](#)
- [\[RDS.37\] Los clústeres de bases de datos Aurora PostgreSQL deberían publicar registros en Logs CloudWatch](#)
- [\[RDS.38\] Las instancias de base de datos de RDS para PostgreSQL deben cifrarse en tránsito](#)
- [\[RDS.39\] Las instancias de base de datos de RDS para MySQL deben cifrarse en tránsito](#)
- [\[RDS.40\] Las instancias de base de datos de RDS para SQL Server deberían publicar los registros en Logs CloudWatch](#)
- [\[RDS.41\] Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito](#)
- [\[RDS.42\] Las instancias de base de datos de RDS para MariaDB deberían publicar registros en Logs CloudWatch](#)
- [\[RDS.44\] El RDS para las instancias de base de datos MariaDB debe cifrarse en tránsito](#)
- [\[Redshift.1\] Los clústeres de Amazon Redshift deberían prohibir el acceso público](#)
- [Las conexiones a los clústeres de Amazon Redshift \[Redshift.2\] deben cifrarse en tránsito](#)
- [Los clústeres de Amazon Redshift \[Redshift.3\] deben tener habilitadas las instantáneas automáticas](#)
- [Los clústeres de Amazon Redshift \[Redshift.4\] deben tener habilitado el registro de auditoría](#)
- [Amazon Redshift \[Redshift.6\] debería tener habilitadas las actualizaciones automáticas a las versiones principales](#)
- [Los clústeres de Redshift \[Redshift.7\] deberían utilizar un enrutamiento de VPC mejorado](#)
- [Los clústeres de Amazon Redshift \[Redshift.8\] no deben usar el nombre de usuario de administrador predeterminado](#)
- [Los clústeres de Redshift \[Redshift.9\] no deben usar el nombre de base de datos predeterminado](#)
- [Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo](#)

- [\[Redshift.11\] Los clústeres de Redshift deben etiquetarse](#)
- [\[Redshift.12\] Las suscripciones a notificaciones de eventos de Redshift deben etiquetarse](#)
- [\[Redshift.13\] Las instantáneas del clúster de Redshift deben etiquetarse](#)
- [\[Redshift.14\] Los grupos de subredes del clúster de Redshift deben etiquetarse](#)
- [\[Redshift.15\] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos](#)
- [\[Redshift.16\] Los grupos de subredes de clústeres de Redshift deben tener subredes de varias zonas de disponibilidad](#)
- [\[Redshift.17\] Los grupos de parámetros del clúster de Redshift deben estar etiquetados](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[RedshiftServerless.3\] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público](#)
- [\[RedshiftServerless.4\] Los espacios de nombres de Redshift Serverless deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado](#)
- [\[RedshiftServerless.6\] Los espacios de nombres de Redshift Serverless deberían exportar los registros a los registros CloudWatch](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de base de datos predeterminado](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.7\] Los buckets de uso general de S3 deben usar la replicación entre regiones](#)
- [\[S3.10\] Los buckets de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida](#)
- [\[S3.11\] Los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos](#)
- [\[S3.12\] no ACLs debe usarse para administrar el acceso de los usuarios a los depósitos de uso general de S3](#)
- [\[S3.13\] Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida](#)

- [\[S3.19\] Los puntos de acceso de S3 deben tener habilitada la configuración de Bloqueo de acceso público](#)
- [\[S3.20\] Los buckets de uso general de S3 deben tener habilitada la eliminación de MFA](#)
- [\[S3.22\] Los buckets de uso general de S3 deben registrar eventos de escritura a nivel de objeto](#)
- [\[S3.23\] Los buckets de uso general de S3 deben registrar eventos de lectura a nivel de objeto](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] las instancias de SageMaker notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook](#)
- [\[SageMaker.4\] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1](#)
- [\[SageMaker.5\] SageMaker los modelos deberían bloquear el tráfico entrante](#)
- [\[SageMaker.6\] Las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas](#)
- [\[SageMaker.7\] SageMaker las imágenes deben estar etiquetadas](#)
- [\[SageMaker.8\] las instancias de SageMaker notebook deberían ejecutarse en plataformas compatibles](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [\[SecretsManager.5\] Los secretos de Secrets Manager deben estar etiquetados](#)
- [\[ServiceCatalog.1\] Las carteras de Service Catalog solo deben compartirse dentro de una AWS organización](#)
- [\[SNS.3\] Los temas de SNS deben etiquetarse](#)
- [\[SNS.4\] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SQS.3\] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público](#)
- [\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)

- [\[SSM.4\] Los documentos SSM no deben ser públicos](#)
- [\[SSM.5\] Los documentos SSM deben estar etiquetados](#)
- [\[StepFunctions.1\] Las máquinas de estado de Step Functions deberían tener el registro activado](#)
- [\[StepFunctions.2\] Las actividades de Step Functions deben estar etiquetadas](#)
- [Los AWS Transfer Family flujos de trabajo de \[Transfer.1\] deben estar etiquetados](#)
- [\[Transfer.2\] Los servidores de Transfer Family no deben utilizar el protocolo FTP para la conexión del punto de conexión](#)
- [\[Transfer.3\] Los conectores Transfer Family deben tener habilitado el registro](#)
- [\[Transfer.4\] Los acuerdos Transfer Family deben estar etiquetados](#)
- [\[Transfer.5\] Los certificados de Transfer Family deben estar etiquetados](#)
- [\[Transfer.6\] Los conectores Transfer Family deben estar etiquetados](#)
- [\[Transfer.7\] Los perfiles de Transfer Family deben estar etiquetados](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas de \[WAF.2\] Regionales AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.4\] Regionales AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [La AWS WAF web de \[WAF.10\] ACLs debe tener al menos una regla o grupo de reglas](#)
- [El registro de ACL AWS WAF web de \[WAF.11\] debe estar habilitado](#)
- [AWS WAF Las reglas de \[WAF.12\] deben tener habilitadas las métricas CloudWatch](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

Asia-Pacífico (Tokio)

Los siguientes controles no se admiten en la región de Asia Pacífico (Tokio).

- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)

- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IoT Twin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)

- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

Canadá (centro)

Los siguientes controles no se admiten en la región de Canadá (Central).

- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)

- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[IoT Twin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Twin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoT Wireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Kinesis.3\] Las transmisiones de Kinesis deben tener un periodo adecuado de retención de datos](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)

- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

Oeste de Canadá (Calgary)

Los siguientes controles no se admiten en la región Canadá Oeste (Calgary).

- [\[ACM.1\] Los certificados importados y emitidos por ACM deben renovarse después de un período de tiempo específico](#)
- [\[ACM.2\] Los certificados RSA administrados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)
- [\[Cuenta.1\] La información de contacto de seguridad debe proporcionarse para un Cuenta de AWS](#)
- [\[Account.2\] Cuentas de AWS debe formar parte de una organización AWS Organizations](#)
- [\[APIGateway.8\] Las rutas de API Gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas V2 de API Gateway](#)
- [\[Amplify.1\] Las aplicaciones de Amplify deben estar etiquetadas](#)
- [\[Amplify.2\] Las ramas de Amplify deben estar etiquetadas](#)
- [\[AppConfig.1\] AWS AppConfig las aplicaciones deben estar etiquetadas](#)
- [\[AppConfig.2\] los perfiles de AWS AppConfig configuración deben estar etiquetados](#)
- [\[AppConfig.3\] AWS AppConfig los entornos deben estar etiquetados](#)
- [\[AppConfig.4\] Las asociaciones AWS AppConfig de extensiones deben estar etiquetadas](#)
- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.2\] AWS AppSync debe tener habilitado el registro a nivel de campo](#)
- [\[AppSync.4\] AWS AppSync APIs GraphQL debe estar etiquetado](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves de API](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[Athena.4\] Los grupos de trabajo de Athena deben tener el registro habilitado](#)

- [\[AutoScaling.2\] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad](#)
- [\[AutoScaling.3\] Las configuraciones de lanzamiento de grupos de Auto Scaling deberían configurar las EC2 instancias para que requieran la versión 2 del Servicio de Metadatos de Instancia \(IMDSv2\)](#)
- [\[AutoScaling.6\] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad](#)
- [\[AutoScaling.9\] Los grupos de Amazon EC2 Auto Scaling deberían usar las plantillas de EC2 lanzamiento de Amazon](#)
- [\[Backup.1\] Los puntos AWS Backup de recuperación deben cifrarse en reposo](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[Batch.1\] Las colas de trabajos por lotes deben estar etiquetadas](#)
- [\[Batch.3\] Los entornos de procesamiento por lotes deben etiquetarse](#)
- [\[Batch.4\] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CloudTrail.6\] Asegurar que los CloudTrail registros del bucket de S3 no son de acceso público](#)
- [\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el bucket de CloudTrail S3](#)

- [\[CloudTrail.10\] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [\[CloudWatch.17\] las acciones CloudWatch de alarma deben estar activadas](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeBuild.1\] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales](#)
- [\[CodeBuild.2\] Las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro](#)
- [\[CodeBuild.3\] Los registros de CodeBuild S3 deben estar cifrados](#)
- [\[CodeBuild.4\] Los entornos de los CodeBuild proyectos deben tener una duración de registro AWS Config](#)
- [\[CodeBuild.7\] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Cognito.1\] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[DataFirehose.1\] Los flujos de entrega de Firehose deben cifrarse en reposo](#)
- [\[DataSync.1\] DataSync las tareas deberían tener el registro activado](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.2\] Los certificados DMS deben estar etiquetados](#)
- [\[DMS.3\] Las suscripciones a eventos de DMS deben estar etiquetadas](#)
- [\[DMS.4\] Las instancias de replicación de DMS deben etiquetarse](#)
- [\[DMS.5\] Los grupos de subredes de replicación del DMS deben estar etiquetados](#)
- [\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)

- [\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)
- [\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado](#)
- [\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DocumentDb.6\] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.6\] Las tablas de DynamoDB deben tener la protección contra eliminación habilitada](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC24\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.21\] La red no ACLs debe permitir la entrada desde 0.0.0/0 al puerto 22 o al puerto 3389](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.25\] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red](#)
- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad](#)

- [\[EC2.33\] Las conexiones de puerta de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.34\] Las tablas de enrutamiento de las puertas de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.40\] Las puertas de enlace de EC2 NAT deben etiquetarse](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben etiquetarse](#)
- [\[EC251\] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)
- [\[EC2.53\] Los grupos EC2 de seguridad no deberían permitir la entrada de 0.0.0.0/0 a los puertos de administración de servidores remotos](#)
- [\[EC2.54\] Los grupos EC2 de seguridad no deberían permitir la entrada de: :/0 a los puertos de administración de servidores remotos](#)
- [\[EC2.55\] VPCs debe configurarse con un punto final de interfaz para la API ECR](#)
- [\[EC2.56\] VPCs debe configurarse con un punto final de interfaz para Docker Registry](#)
- [\[EC2.57\] VPCs debe configurarse con un punto final de interfaz para Systems Manager](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.170\] Las plantillas de EC2 lanzamiento deben usar el servicio de metadatos de instancias versión 2 \(\) IMDSv2](#)
- [\[EC2.171\] Las conexiones EC2 VPN deben tener el registro habilitado](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.175\] Las plantillas de EC2 lanzamiento deben estar etiquetadas](#)
- [\[EC2.177\] las sesiones espejo EC2 de tráfico deberían estar etiquetadas](#)
- [\[EC2.179\] Los objetivos EC2 de tráfico reflejados deben estar etiquetados](#)
- [\[ECR.1\] Los repositorios privados del ECR deben tener configurado el escaneo de imágenes](#)
- [\[ECR.2\] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas](#)
- [\[ECR.3\] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[ECR.5\] Los repositorios de ECR deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [\[ECS.3\] Las definiciones de tareas de ECS no deben compartir el espacio de nombres de los procesos del anfitrión](#)

- [\[ECS.4\] Los contenedores de ECS deben ejecutarse sin privilegios](#)
- [\[ECS.5\] Los contenedores ECS deben limitarse al acceso de solo lectura a los sistemas de archivos raíz](#)
- [\[ECS.8\] Los secretos no deben pasarse como variables de entorno del contenedor](#)
- [\[ECS.9\] Las definiciones de tareas de ECS deben tener una configuración de registro](#)
- [\[ECS.10\] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate](#)
- [\[ECS.12\] Los clústeres de ECS deben usar Container Insights](#)
- [\[ECS.16\] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas](#)
- [\[ECS.17\] Las definiciones de tareas de ECS no deben utilizar el modo de red host](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] Los volúmenes de Amazon EFS deben estar en los planes de respaldo](#)
- [\[EFS.3\] Los puntos de acceso EFS deben aplicar un directorio raíz](#)
- [\[EFS.4\] Los puntos de acceso EFS deben imponer una identidad de usuario](#)
- [\[EFS.6\] Los destinos de montaje de EFS no deben estar asociados a una subred pública](#)
- [\[EFS.7\] Los sistemas de archivos de EFS deben tener habilitadas las copias de seguridad automáticas](#)
- [\[EFS.8\] Los sistemas de archivos de EFS deben cifrarse en reposo](#)
- [\[EKS.2\] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible](#)
- [\[EKS.3\] Los clústeres de EKS deben usar secretos de Kubernetes cifrados](#)
- [\[EKS.6\] Los clústeres de EKS deben etiquetarse](#)
- [\[EKS.7\] Las configuraciones de los proveedores de identidad de EKS deben etiquetarse](#)
- [\[EKS.8\] Los clústeres de EKS deben tener habilitado el registro de auditoría](#)
- [\[ELB.2\] Los equilibradores de carga clásicos con agentes de escucha SSL/HTTPS deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.10\] Equilibrador de carga clásico debe abarcar varias zonas de disponibilidad](#)
- [\[ELB.12\] Equilibrador de carga de aplicación debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.13\] Los equilibradores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad](#)

- [\[ELB.14\] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.17\] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.2\] ElastiCache Los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias](#)
- [\[ElastiCache.3\] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática](#)
- [\[ElastiCache.4\] los grupos de ElastiCache replicación deben estar cifrados en reposo](#)
- [\[ElastiCache.5\] los grupos de ElastiCache replicación deben cifrarse en tránsito](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)
- [\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)
- [\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)
- [\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)
- [\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)
- [\[EMR.2\] La configuración de bloqueo del acceso público de Amazon EMR debe estar habilitada](#)
- [\[EMR.3\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo](#)
- [\[ES.3\] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos](#)
- [\[ES.4\] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros](#)
- [\[EventBridge.3\] Los autobuses de eventos EventBridge personalizados deben incluir una política basada en los recursos](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)

- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FSx.1\] en el caso FSx de OpenZFS, los sistemas de archivos deben configurarse para copiar etiquetas en copias de seguridad y volúmenes](#)
- [\[FSx.2\] FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad](#)
- [\[FSx.3\] FSx para los sistemas de archivos OpenZFS, debe configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[FSx.4\] FSx para los sistemas de archivos NetApp ONTAP, debe configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[FSx.5\] FSx para Windows, los sistemas de archivos del servidor de archivos deben configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[Glue.3\] Las transformaciones AWS Glue de aprendizaje automático deben cifrarse en reposo](#)
- [\[Glue.4\] Los trabajos de AWS Glue Spark deberían ejecutarse en versiones compatibles de AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[GuardDuty.3\] GuardDuty IPSets debe estar etiquetado](#)
- [\[GuardDuty.5\] La supervisión de registros de auditoría de GuardDuty EKS debe estar habilitada](#)
- [\[GuardDuty.6\] La protección de GuardDuty Lambda debe estar habilitada](#)
- [\[GuardDuty.7\] La supervisión en tiempo de ejecución de GuardDuty EKS debe estar habilitada](#)
- [\[GuardDuty.8\] La protección contra GuardDuty malware para EC2 debe estar habilitada](#)
- [\[GuardDuty.9\] La protección de GuardDuty RDS debe estar habilitada](#)
- [\[GuardDuty.10\] La protección de GuardDuty S3 debe estar habilitada](#)
- [\[GuardDuty.11\] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada](#)
- [\[GuardDuty.12\] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada](#)
- [\[GuardDuty.13\] La monitorización del GuardDuty EC2 tiempo de ejecución debe estar habilitada](#)
- [\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)
- [\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)
- [\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)
- [\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)

- [\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)
- [\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)
- [\[IAM.7\] Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)
- [\[IAM.10\] Las políticas de contraseñas de usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.11\] Asegurar que la política de contraseñas de IAM requiera al menos una letra mayúscula](#)
- [\[IAM.12\] Asegurar que la política de contraseñas de IAM requiera al menos una letra minúscula](#)
- [\[IAM.13\] Asegurar que la política de contraseñas de IAM requiera al menos un símbolo](#)
- [\[IAM.14\] Asegurar que la política de contraseñas de IAM requiera al menos un número](#)
- [\[IAM.15\] Asegurar que la política de contraseñas de IAM requiera una longitud mínima de 14 o más](#)
- [\[IAM.16\] Asegurar que la política de contraseñas de IAM impida la reutilización de contraseñas](#)
- [\[IAM.17\] Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos](#)
- [\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)
- [\[IAM.19\] MFA se debe habilitar para todos los usuarios de IAM](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)
- [\[IAM.22\] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días](#)
- [\[IAM.24\] Los roles de IAM deben etiquetarse](#)
- [\[IAM.25\] Los usuarios de IAM deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IAM.27\] Las identidades de IAM no deben tener adjunta la política AWSCloud ShellFullAccess](#)
- [\[IAM.28\] El analizador de acceso externo del Analizador de acceso de IAM debe habilitarse](#)
- [\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.2\] El análisis de ECR en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)

- [\[Inspector.4\] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado](#)
- [Los perfiles de AWS IoT Device Defender seguridad \[IoT.1\] deben estar etiquetados](#)
- [\[IoT.2\] las acciones de AWS IoT Core mitigación deben estar etiquetadas](#)
- [AWS IoT Core Las dimensiones de \[IoT.3\] deben estar etiquetadas](#)
- [Los AWS IoT Core autorizadores \[IoT.4\] deben estar etiquetados](#)
- [Los alias de los AWS IoT Core roles \[IoT.5\] deben estar etiquetados](#)
- [AWS IoT Core Las políticas \[IoT.6\] deben estar etiquetadas](#)
- [\[IoT Events .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoT Events .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Events .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Site Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Site Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Twin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoT Wireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)
- [\[Kinesis.1\] Las transmisiones de Kinesis deben cifrarse en reposo](#)
- [\[Kinesis.2\] Las transmisiones de Kinesis deben etiquetarse](#)
- [\[Kinesis.3\] Las transmisiones de Kinesis deben tener un periodo adecuado de retención de datos](#)
- [\[KMS.1\] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS](#)

- [\[KMS.2\] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.5\] Las claves KMS no deben ser de acceso público](#)
- [\[Lambda.5\] Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)
- [\[MQ.2\] Los corredores de ActiveMQ deberían transmitir los registros de auditoría a CloudWatch](#)
- [\[MQ.3\] Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[MQ.4\] Los agentes de Amazon MQ deben estar etiquetados](#)
- [\[MQ.5\] Los corredores ActiveMQ deben usar el modo de implementación activo/en espera](#)
- [\[MQ.6\] Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres](#)
- [\[MSK.1\] Los clústeres de MSK deben cifrarse en tránsito entre los nodos intermediarios](#)
- [\[MSK.2\] Los clústeres de MSK deberían tener configurada una supervisión mejorada](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [\[Neptune.4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación](#)
- [\[Neptune.5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas](#)
- [\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM](#)
- [\[Neptune.8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas](#)
- [\[Neptune.9\] Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad](#)
- [Los NetworkFirewall firewalls de Network Firewall se deben implementar en varias zonas de disponibilidad](#)

- [\[NetworkFirewall.2\] El registro de Network Firewall debe estar habilitado](#)
- [\[NetworkFirewall.3\] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas](#)
- [\[NetworkFirewall.4\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos](#)
- [\[NetworkFirewall.5\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados](#)
- [El grupo de reglas de Stateless Network Firewall \[NetworkFirewall.6\] no debe estar vacío](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de eliminación](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de cambio de subred](#)
- [Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)
- [Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)
- [Los OpenSearch dominios \[Opensearch.3\] deben cifrar los datos enviados entre nodos](#)
- [El registro de errores de OpenSearch dominio \[Opensearch.4\] en CloudWatch Logs debe estar activado](#)
- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)
- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los OpenSearch dominios \[Opensearch.7\] deben tener habilitado un control de acceso detallado](#)
- [\[Opensearch.8\] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente](#)
- [Los OpenSearch dominios \[Opensearch.9\] deben estar etiquetados](#)
- [Los OpenSearch dominios \[Opensearch.10\] deben tener instalada la última actualización de software](#)
- [Los OpenSearch dominios \[Opensearch.11\] deben tener al menos tres nodos principales dedicados](#)
- [La autoridad emisora de certificados AWS Private CA raíz \[PCA.1\] debe estar deshabilitada](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [Las instancias de RDS \[RDS.18\] deben implementarse en una VPC](#)

- [Los clústeres de bases de datos de RDS \[RDS.24\] deben usar un nombre de usuario de administrador personalizado](#)
- [Las instancias de bases de datos de RDS \[RDS.25\] deben usar un nombre de usuario de administrador personalizado](#)
- [Las instancias de base de datos de RDS \[RDS.26\] deben protegerse mediante un plan de copias de seguridad](#)
- [Los clústeres de bases de datos de RDS \[RDS.27\] deben cifrarse en reposo](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.34\] Los clústeres de bases de datos Aurora MySQL deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[RDS.36\] Las instancias de base de datos de RDS para PostgreSQL deben publicar registros en Logs CloudWatch](#)
- [\[RDS.37\] Los clústeres de bases de datos Aurora PostgreSQL deberían publicar registros en Logs CloudWatch](#)
- [\[RDS.38\] Las instancias de base de datos de RDS para PostgreSQL deben cifrarse en tránsito](#)
- [\[RDS.39\] Las instancias de base de datos de RDS para MySQL deben cifrarse en tránsito](#)
- [\[RDS.40\] Las instancias de base de datos de RDS para SQL Server deberían publicar los registros en Logs CloudWatch](#)
- [\[RDS.41\] Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito](#)
- [\[RDS.42\] Las instancias de base de datos de RDS para MariaDB deberían publicar registros en Logs CloudWatch](#)
- [\[RDS.44\] El RDS para las instancias de base de datos MariaDB debe cifrarse en tránsito](#)
- [Los clústeres de Amazon Redshift \[Redshift.3\] deben tener habilitadas las instantáneas automáticas](#)
- [Amazon Redshift \[Redshift.6\] debería tener habilitadas las actualizaciones automáticas a las versiones principales](#)
- [Los clústeres de Redshift \[Redshift.7\] deberían utilizar un enrutamiento de VPC mejorado](#)
- [Los clústeres de Amazon Redshift \[Redshift.8\] no deben usar el nombre de usuario de administrador predeterminado](#)
- [Los clústeres de Redshift \[Redshift.9\] no deben usar el nombre de base de datos predeterminado](#)

- [Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo](#)
- [\[Redshift.15\] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos](#)
- [\[Redshift.16\] Los grupos de subredes de clústeres de Redshift deben tener subredes de varias zonas de disponibilidad](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[RedshiftServerless.3\] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público](#)
- [\[RedshiftServerless.4\] Los espacios de nombres de Redshift Serverless deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado](#)
- [\[RedshiftServerless.6\] Los espacios de nombres de Redshift Serverless deberían exportar los registros a los registros CloudWatch](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de base de datos predeterminado](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.7\] Los buckets de uso general de S3 deben usar la replicación entre regiones](#)
- [\[S3.10\] Los buckets de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida](#)
- [\[S3.11\] Los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos](#)
- [\[S3.12\] no ACLs debe usarse para administrar el acceso de los usuarios a los depósitos de uso general de S3](#)
- [\[S3.13\] Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida](#)
- [\[S3.19\] Los puntos de acceso de S3 deben tener habilitada la configuración de Bloqueo de acceso público](#)
- [\[S3.20\] Los buckets de uso general de S3 deben tener habilitada la eliminación de MFA](#)
- [\[S3.22\] Los buckets de uso general de S3 deben registrar eventos de escritura a nivel de objeto](#)

- [\[S3.23\] Los buckets de uso general de S3 deben registrar eventos de lectura a nivel de objeto](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] las instancias de SageMaker notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook](#)
- [\[SageMaker.4\] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1](#)
- [\[SageMaker.5\] SageMaker los modelos deberían bloquear el tráfico entrante](#)
- [\[SageMaker.6\] Las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas](#)
- [\[SageMaker.7\] SageMaker las imágenes deben estar etiquetadas](#)
- [\[SageMaker.8\] las instancias de SageMaker notebook deberían ejecutarse en plataformas compatibles](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [\[ServiceCatalog.1\] Las carteras de Service Catalog solo deben compartirse dentro de una AWS organización](#)
- [\[SNS.4\] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SQS.3\] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público](#)
- [\[SSM.2\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de parche de COMPLIANT después de la instalación de un parche](#)
- [\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [\[SSM.4\] Los documentos SSM no deben ser públicos](#)
- [\[StepFunctions.1\] Las máquinas de estado de Step Functions deberían tener el registro activado](#)
- [\[Transfer.2\] Los servidores de Transfer Family no deben utilizar el protocolo FTP para la conexión del punto de conexión](#)

- [\[Transfer.3\] Los conectores Transfer Family deben tener habilitado el registro](#)
- [\[Transfer.4\] Los acuerdos Transfer Family deben estar etiquetados](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas de \[WAF.2\] Regionales AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.4\] Regionales AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [La AWS WAF web de \[WAF.10\] ACLs debe tener al menos una regla o grupo de reglas](#)
- [El registro de ACL AWS WAF web de \[WAF.11\] debe estar habilitado](#)
- [AWS WAF Las reglas de \[WAF.12\] deben tener habilitadas las métricas CloudWatch](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

China (Pekín)

Los siguientes controles no se admiten en la región China (Pekín).

- [\[ACM.1\] Los certificados importados y emitidos por ACM deben renovarse después de un período de tiempo específico](#)
- [\[ACM.2\] Los certificados RSA administrados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)
- [\[Account.2\] Cuentas de AWS debe formar parte de una organización AWS Organizations](#)
- [\[APIGateway.2\] Las etapas de la API de REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend](#)
- [\[Amplify.1\] Las aplicaciones de Amplify deben estar etiquetadas](#)
- [\[Amplify.2\] Las ramas de Amplify deben estar etiquetadas](#)
- [\[AppConfig.1\] AWS AppConfig las aplicaciones deben estar etiquetadas](#)
- [\[AppConfig.2\] los perfiles de AWS AppConfig configuración deben estar etiquetados](#)

- [\[AppConfig.3\] AWS AppConfig los entornos deben estar etiquetados](#)
- [\[AppConfig.4\] Las asociaciones AWS AppConfig de extensiones deben estar etiquetadas](#)
- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[AutoScaling.10\] Los grupos EC2 de Auto Scaling deben estar etiquetados](#)
- [\[Backup.1\] Los puntos AWS Backup de recuperación deben cifrarse en reposo](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[Batch.1\] Las colas de trabajos por lotes deben estar etiquetadas](#)
- [\[Batch.2\] Las políticas de programación de lotes deben estar etiquetadas](#)
- [\[Batch.3\] Los entornos de procesamiento por lotes deben etiquetarse](#)
- [\[Batch.4\] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CloudTrail.10\] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el cliente AWS KMS keys](#)

- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Cognito.1\] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[DataFirehose.1\] Los flujos de entrega de Firehose deben cifrarse en reposo](#)
- [\[DataSync.2\] DataSync las tareas deben estar etiquetadas](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.4\] Las instancias de replicación de DMS deben etiquetarse](#)
- [\[DMS.5\] Los grupos de subredes de replicación del DMS deben estar etiquetados](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado](#)
- [\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)

- [\[EC215\] EC2 Las subredes de Amazon no deben asignar automáticamente direcciones IP públicas](#)
- [\[EC2.16\] Deben eliminarse las listas de control de acceso a la red no utilizadas](#)
- [\[EC220\] Ambos túneles de VPN de una conexión de AWS Site-to-Site VPN deben estar activos](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad](#)
- [\[EC2.33\] Las conexiones de puerta de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.34\] Las tablas de enrutamiento de las puertas de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.35\] Las interfaces EC2 de red deben etiquetarse](#)
- [\[EC2.36\] Las pasarelas de EC2 clientes deben estar etiquetadas](#)
- [\[EC2.40\] Las puertas de enlace de EC2 NAT deben etiquetarse](#)
- [La EC2 red \[EC2.41\] ACLs debe estar etiquetada](#)
- [\[EC2.42\] Las tablas de EC2 enrutamiento deben estar etiquetadas](#)
- [\[EC2.43\] los grupos EC2 de seguridad deben estar etiquetados](#)
- [EC2 Las subredes \[EC2.44\] deben estar etiquetadas](#)
- [\[EC2.46\] Amazon VPCs debería estar etiquetado](#)
- [\[EC2.47\] Los servicios de puntos de conexión de Amazon VPC deben etiquetarse](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben etiquetarse](#)
- [\[EC2.49\] Las conexiones de emparejamiento de Amazon VPC deben etiquetarse](#)
- [\[EC251\] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)
- [\[EC2.53\] Los grupos EC2 de seguridad no deberían permitir la entrada de 0.0.0.0/0 a los puertos de administración de servidores remotos](#)
- [\[EC2.54\] Los grupos EC2 de seguridad no deberían permitir la entrada de: :/0 a los puertos de administración de servidores remotos](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.171\] Las conexiones EC2 VPN deben tener el registro habilitado](#)

- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.174\] Los conjuntos de opciones de EC2 DHCP deben estar etiquetados](#)
- [\[EC2.175\] Las plantillas de EC2 lanzamiento deben estar etiquetadas](#)
- [\[EC2.176\] Las listas de EC2 prefijos deben estar etiquetadas](#)
- [\[EC2.177\] las sesiones espejo EC2 de tráfico deberían estar etiquetadas](#)
- [\[EC2.178\] Los filtros espejo de EC2 tráfico deben estar etiquetados](#)
- [\[EC2.179\] Los objetivos EC2 de tráfico reflejados deben estar etiquetados](#)
- [\[ECR.1\] Los repositorios privados del ECR deben tener configurado el escaneo de imágenes](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[ECS.13\] Los servicios de ECS deben estar etiquetados](#)
- [\[ECS.15\] Las definiciones de tareas de ECS deben etiquetarse](#)
- [\[EFS.6\] Los destinos de montaje de EFS no deben estar asociados a una subred pública](#)
- [\[EKS.3\] Los clústeres de EKS deben usar secretos de Kubernetes cifrados](#)
- [\[EKS.6\] Los clústeres de EKS deben etiquetarse](#)
- [\[EKS.7\] Las configuraciones de los proveedores de identidad de EKS deben etiquetarse](#)
- [\[ELB.2\] Los equilibradores de carga clásicos con agentes de escucha SSL/HTTPS deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.16\] Los equilibradores de carga de aplicaciones deben estar asociados a una ACL web de AWS WAF](#)
- [\[ELB.17\] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)
- [\[EMR.2\] La configuración de bloqueo del acceso público de Amazon EMR debe estar habilitada](#)
- [\[EMR.3\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo](#)
- [\[EMR.4\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito](#)
- [\[ES.4\] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)

- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FSx.1\] en el caso FSx de OpenZFS, los sistemas de archivos deben configurarse para copiar etiquetas en copias de seguridad y volúmenes](#)
- [\[FSx.2\] FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad](#)
- [\[FSx.5\] FSx para Windows, los sistemas de archivos del servidor de archivos deben configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[GuardDuty.3\] GuardDuty IPSets debe estar etiquetado](#)
- [\[GuardDuty.4\] GuardDuty los detectores deben estar etiquetados](#)
- [\[GuardDuty.5\] La supervisión de registros de auditoría de GuardDuty EKS debe estar habilitada](#)
- [\[GuardDuty.6\] La protección de GuardDuty Lambda debe estar habilitada](#)
- [\[GuardDuty.7\] La supervisión en tiempo de ejecución de GuardDuty EKS debe estar habilitada](#)
- [\[GuardDuty.8\] La protección contra GuardDuty malware para EC2 debe estar habilitada](#)
- [\[GuardDuty.9\] La protección de GuardDuty RDS debe estar habilitada](#)
- [\[GuardDuty.10\] La protección de GuardDuty S3 debe estar habilitada](#)
- [\[GuardDuty.11\] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada](#)
- [\[GuardDuty.12\] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada](#)
- [\[GuardDuty.13\] La monitorización del GuardDuty EC2 tiempo de ejecución debe estar habilitada](#)
- [\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)
- [\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)
- [\[IAM.23\] Los analizadores del Analizador de acceso de IAM deben etiquetarse](#)
- [\[IAM.24\] Los roles de IAM deben etiquetarse](#)
- [\[IAM.25\] Los usuarios de IAM deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)

- [\[IAM.27\] Las identidades de IAM no deben tener adjunta la política AWSCloud ShellFullAccess](#)
- [\[IAM.28\] El analizador de acceso externo del Analizador de acceso de IAM debe habilitarse](#)
- [\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.2\] El análisis de ECR en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.4\] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[IoT Events .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoT Events .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Events .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Site Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Site Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Twin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoT Wireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)
- [\[MQ.2\] Los corredores de ActiveMQ deberían transmitir los registros de auditoría a CloudWatch](#)
- [\[MQ.4\] Los agentes de Amazon MQ deben estar etiquetados](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)

- [\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [\[Neptune.4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación](#)
- [\[Neptune.5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas](#)
- [\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM](#)
- [\[Neptune.8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas](#)
- [\[Neptune.9\] Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad](#)
- [Los NetworkFirewall firewalls de Network Firewall se deben implementar en varias zonas de disponibilidad](#)
- [\[NetworkFirewall.2\] El registro de Network Firewall debe estar habilitado](#)
- [\[NetworkFirewall.3\] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas](#)
- [\[NetworkFirewall.4\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos](#)
- [\[NetworkFirewall.5\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados](#)
- [El grupo de reglas de Stateless Network Firewall \[NetworkFirewall.6\] no debe estar vacío](#)
- [Los NetworkFirewall firewalls de Network Firewall se deben etiquetar](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de eliminación](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de cambio de subred](#)
- [Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)
- [Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)

- [Los OpenSearch dominios \[Opensearch.3\] deben cifrar los datos enviados entre nodos](#)
- [El registro de errores de OpenSearch dominio \[Opensearch.4\] en CloudWatch Logs debe estar activado](#)
- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)
- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los OpenSearch dominios \[Opensearch.7\] deben tener habilitado un control de acceso detallado](#)
- [\[Opensearch.8\] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente](#)
- [Los OpenSearch dominios \[Opensearch.11\] deben tener al menos tres nodos principales dedicados](#)
- [La autoridad emisora de certificados AWS Private CA raíz \[PCA.1\] debe estar deshabilitada](#)
- [\[PCA.2\] Se debe etiquetar a las autoridades certificadoras de CA AWS privadas](#)
- [Los clústeres de RDS \[RDS.7\] deben tener habilitada la protección contra la eliminación](#)
- [La autenticación de IAM \[RDS.10\] debe configurarse para las instancias de RDS](#)
- [La autenticación de IAM \[RDS.12\] debe configurarse para los clústeres de RDS](#)
- [Las actualizaciones automáticas de las versiones secundarias de RDS \[RDS.13\] deben estar habilitadas](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [Los clústeres de bases de datos de RDS \[RDS.15\] deben configurarse para varias zonas de disponibilidad](#)
- [Los clústeres de bases de datos de RDS \[RDS.16\] deben configurarse para copiar etiquetas en las instantáneas](#)
- [Los clústeres de bases de datos de RDS \[RDS.24\] deben usar un nombre de usuario de administrador personalizado](#)
- [Las instancias de bases de datos de RDS \[RDS.25\] deben usar un nombre de usuario de administrador personalizado](#)
- [Las instancias de base de datos de RDS \[RDS.26\] deben protegerse mediante un plan de copias de seguridad](#)
- [Los clústeres de bases de datos de RDS \[RDS.27\] deben cifrarse en reposo](#)
- [\[RDS.28\] Los clústeres de base de datos de RDS deben etiquetarse](#)
- [\[RDS.29\] Las instantáneas del clúster de base de datos de RDS deben etiquetarse](#)

- [\[RDS.30\] Las instancias de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.32\] Las instantáneas de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.33\] Los grupos de subredes de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.34\] Los clústeres de bases de datos Aurora MySQL deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[RDS.37\] Los clústeres de bases de datos Aurora PostgreSQL deberían publicar registros en Logs CloudWatch](#)
- [\[RDS.42\] Las instancias de base de datos de RDS para MariaDB deberían publicar registros en Logs CloudWatch](#)
- [\[RDS.44\] El RDS para las instancias de base de datos MariaDB debe cifrarse en tránsito](#)
- [Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo](#)
- [\[Redshift.14\] Los grupos de subredes del clúster de Redshift deben etiquetarse](#)
- [\[Redshift.15\] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos](#)
- [\[Redshift.17\] Los grupos de parámetros del clúster de Redshift deben estar etiquetados](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[RedshiftServerless.3\] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.22\] Los buckets de uso general de S3 deben registrar eventos de escritura a nivel de objeto](#)
- [\[S3.23\] Los buckets de uso general de S3 deben registrar eventos de lectura a nivel de objeto](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)

- [\[SageMaker.4\] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1](#)
- [\[SageMaker.5\] SageMaker los modelos deberían bloquear el tráfico entrante](#)
- [\[SageMaker.6\] Las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas](#)
- [\[SageMaker.7\] SageMaker las imágenes deben estar etiquetadas](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [\[ServiceCatalog.1\] Las carteras de Service Catalog solo deben compartirse dentro de una AWS organización](#)
- [\[SSM.5\] Los documentos SSM deben estar etiquetados](#)
- [\[Transfer.2\] Los servidores de Transfer Family no deben utilizar el protocolo FTP para la conexión del punto de conexión](#)
- [\[Transfer.4\] Los acuerdos Transfer Family deben estar etiquetados](#)
- [\[Transfer.5\] Los certificados de Transfer Family deben estar etiquetados](#)
- [\[Transfer.6\] Los conectores Transfer Family deben estar etiquetados](#)
- [\[Transfer.7\] Los perfiles de Transfer Family deben estar etiquetados](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

China (Ningxia)

Los siguientes controles no se admiten en la región China (Ningxia).

- [\[ACM.1\] Los certificados importados y emitidos por ACM deben renovarse después de un período de tiempo específico](#)

- [\[ACM.2\] Los certificados RSA administrados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)
- [\[Account.2\] Cuentas de AWS debe formar parte de una organización AWS Organizations](#)
- [\[APIGateway.2\] Las etapas de la API de REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend](#)
- [\[Amplify.1\] Las aplicaciones de Amplify deben estar etiquetadas](#)
- [\[Amplify.2\] Las ramas de Amplify deben estar etiquetadas](#)
- [\[AppConfig.1\] AWS AppConfig las aplicaciones deben estar etiquetadas](#)
- [\[AppConfig.2\] los perfiles de AWS AppConfig configuración deben estar etiquetados](#)
- [\[AppConfig.3\] AWS AppConfig los entornos deben estar etiquetados](#)
- [\[AppConfig.4\] Las asociaciones AWS AppConfig de extensiones deben estar etiquetadas](#)
- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[AutoScaling.10\] Los grupos EC2 de Auto Scaling deben estar etiquetados](#)
- [\[Backup.1\] Los puntos AWS Backup de recuperación deben cifrarse en reposo](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[Batch.1\] Las colas de trabajos por lotes deben estar etiquetadas](#)
- [\[Batch.2\] Las políticas de programación de lotes deben estar etiquetadas](#)
- [\[Batch.3\] Los entornos de procesamiento por lotes deben etiquetarse](#)
- [\[Batch.4\] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)

- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CloudTrail.10\] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Cognito.1\] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[DataFirehose.1\] Los flujos de entrega de Firehose deben cifrarse en reposo](#)
- [\[DataSync.2\] DataSync las tareas deben estar etiquetadas](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.4\] Las instancias de replicación de DMS deben etiquetarse](#)
- [\[DMS.5\] Los grupos de subredes de replicación del DMS deben estar etiquetados](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado](#)
- [\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)

- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC215\] EC2 Las subredes de Amazon no deben asignar automáticamente direcciones IP públicas](#)
- [\[EC2.16\] Deben eliminarse las listas de control de acceso a la red no utilizadas](#)
- [\[EC220\] Ambos túneles de VPN de una conexión de AWS Site-to-Site VPN deben estar activos](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad](#)
- [\[EC2.33\] Las conexiones de puerta de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.34\] Las tablas de enrutamiento de las puertas de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.35\] Las interfaces EC2 de red deben etiquetarse](#)
- [\[EC2.36\] Las pasarelas de EC2 clientes deben estar etiquetadas](#)
- [\[EC2.40\] Las puertas de enlace de EC2 NAT deben etiquetarse](#)
- [La EC2 red \[EC2.41\] ACLs debe estar etiquetada](#)
- [\[EC2.42\] Las tablas de EC2 enrutamiento deben estar etiquetadas](#)
- [\[EC2.43\] los grupos EC2 de seguridad deben estar etiquetados](#)
- [EC2 Las subredes \[EC2.44\] deben estar etiquetadas](#)
- [\[EC2.46\] Amazon VPCs debería estar etiquetado](#)
- [\[EC2.47\] Los servicios de puntos de conexión de Amazon VPC deben etiquetarse](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben etiquetarse](#)
- [\[EC2.49\] Las conexiones de emparejamiento de Amazon VPC deben etiquetarse](#)
- [\[EC2.50\] Las puertas de enlace de EC2 VPN deben etiquetarse](#)
- [\[EC251\] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)

- [\[EC2.171\] Las conexiones EC2 VPN deben tener el registro habilitado](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.174\] Los conjuntos de opciones de EC2 DHCP deben estar etiquetados](#)
- [\[EC2.175\] Las plantillas de EC2 lanzamiento deben estar etiquetadas](#)
- [\[EC2.176\] Las listas de EC2 prefijos deben estar etiquetadas](#)
- [\[EC2.177\] las sesiones espejo EC2 de tráfico deberían estar etiquetadas](#)
- [\[EC2.178\] Los filtros espejo de EC2 tráfico deben estar etiquetados](#)
- [\[EC2.179\] Los objetivos EC2 de tráfico reflejados deben estar etiquetados](#)
- [\[ECR.1\] Los repositorios privados del ECR deben tener configurado el escaneo de imágenes](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[ECS.13\] Los servicios de ECS deben estar etiquetados](#)
- [\[ECS.15\] Las definiciones de tareas de ECS deben etiquetarse](#)
- [\[EFS.3\] Los puntos de acceso EFS deben aplicar un directorio raíz](#)
- [\[EFS.4\] Los puntos de acceso EFS deben imponer una identidad de usuario](#)
- [\[EFS.6\] Los destinos de montaje de EFS no deben estar asociados a una subred pública](#)
- [\[EKS.3\] Los clústeres de EKS deben usar secretos de Kubernetes cifrados](#)
- [\[EKS.6\] Los clústeres de EKS deben etiquetarse](#)
- [\[EKS.7\] Las configuraciones de los proveedores de identidad de EKS deben etiquetarse](#)
- [\[ELB.2\] Los equilibradores de carga clásicos con agentes de escucha SSL/HTTPS deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.16\] Los equilibradores de carga de aplicaciones deben estar asociados a una ACL web de AWS WAF](#)
- [\[ELB.17\] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)
- [\[EMR.2\] La configuración de bloqueo del acceso público de Amazon EMR debe estar habilitada](#)
- [\[EMR.3\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo](#)
- [\[EMR.4\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito](#)

- [\[ES.4\] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FSx.1\] en el caso FSx de OpenZFS, los sistemas de archivos deben configurarse para copiar etiquetas en copias de seguridad y volúmenes](#)
- [\[FSx.2\] FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad](#)
- [\[FSx.5\] FSx para Windows, los sistemas de archivos del servidor de archivos deben configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[Glue.3\] Las transformaciones AWS Glue de aprendizaje automático deben cifrarse en reposo](#)
- [\[GuardDuty.3\] GuardDuty IPSets debe estar etiquetado](#)
- [\[GuardDuty.4\] GuardDuty los detectores deben estar etiquetados](#)
- [\[GuardDuty.5\] La supervisión de registros de auditoría de GuardDuty EKS debe estar habilitada](#)
- [\[GuardDuty.6\] La protección de GuardDuty Lambda debe estar habilitada](#)
- [\[GuardDuty.7\] La supervisión en tiempo de ejecución de GuardDuty EKS debe estar habilitada](#)
- [\[GuardDuty.8\] La protección contra GuardDuty malware para EC2 debe estar habilitada](#)
- [\[GuardDuty.9\] La protección de GuardDuty RDS debe estar habilitada](#)
- [\[GuardDuty.10\] La protección de GuardDuty S3 debe estar habilitada](#)
- [\[GuardDuty.11\] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada](#)
- [\[GuardDuty.12\] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada](#)
- [\[GuardDuty.13\] La monitorización del GuardDuty EC2 tiempo de ejecución debe estar habilitada](#)
- [\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)
- [\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)

- [\[IAM.23\] Los analizadores del Analizador de acceso de IAM deben etiquetarse](#)
- [\[IAM.24\] Los roles de IAM deben etiquetarse](#)
- [\[IAM.25\] Los usuarios de IAM deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IAM.27\] Las identidades de IAM no deben tener adjunta la política AWS Cloud Shell FullAccess](#)
- [\[IAM.28\] El analizador de acceso externo del Analizador de acceso de IAM debe habilitarse](#)
- [\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.2\] El análisis de ECR en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.4\] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[IoT Events .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoT Events .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Events .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Site Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Site Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Twin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoT Wireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)
- [\[Lambda.1\] Las políticas de función de Lambda deberían prohibir el acceso público](#)

- [\[Lambda.2\] Las funciones de Lambda deben usar los tiempos de ejecución admitidos](#)
- [\[Lambda.3\] Las funciones de Lambda deben estar en una VPC](#)
- [\[Lambda.5\] Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad](#)
- [\[Lambda.6\] Las funciones de Lambda deben estar etiquetadas](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)
- [\[MQ.2\] Los corredores de ActiveMQ deberían transmitir los registros de auditoría a CloudWatch](#)
- [\[MQ.4\] Los agentes de Amazon MQ deben estar etiquetados](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [Los NetworkFirewall firewalls de Network Firewall se deben implementar en varias zonas de disponibilidad](#)
- [\[NetworkFirewall.2\] El registro de Network Firewall debe estar habilitado](#)
- [\[NetworkFirewall.3\] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas](#)
- [\[NetworkFirewall.4\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos](#)
- [\[NetworkFirewall.5\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados](#)
- [El grupo de reglas de Stateless Network Firewall \[NetworkFirewall.6\] no debe estar vacío](#)
- [Los NetworkFirewall firewalls de Network Firewall se deben etiquetar](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de eliminación](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de cambio de subred](#)
- [Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)
- [Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)
- [Los OpenSearch dominios \[Opensearch.3\] deben cifrar los datos enviados entre nodos](#)
- [El registro de errores de OpenSearch dominio \[Opensearch.4\] en CloudWatch Logs debe estar activado](#)
- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)

- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los OpenSearch dominios \[Opensearch.7\] deben tener habilitado un control de acceso detallado](#)
- [\[Opensearch.8\] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente](#)
- [Los OpenSearch dominios \[Opensearch.11\] deben tener al menos tres nodos principales dedicados](#)
- [La autoridad emisora de certificados AWS Private CA raíz \[PCA.1\] debe estar deshabilitada](#)
- [\[PCA.2\] Se debe etiquetar a las autoridades certificadoras de CA AWS privadas](#)
- [Los clústeres de RDS \[RDS.7\] deben tener habilitada la protección contra la eliminación](#)
- [\[RDS.9\] Las instancias de base de datos de RDS deben publicar los registros en Logs CloudWatch](#)
- [La autenticación de IAM \[RDS.10\] debe configurarse para las instancias de RDS](#)
- [La autenticación de IAM \[RDS.12\] debe configurarse para los clústeres de RDS](#)
- [Las actualizaciones automáticas de las versiones secundarias de RDS \[RDS.13\] deben estar habilitadas](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [Los clústeres de bases de datos de RDS \[RDS.15\] deben configurarse para varias zonas de disponibilidad](#)
- [Los clústeres de bases de datos de RDS \[RDS.24\] deben usar un nombre de usuario de administrador personalizado](#)
- [Las instancias de bases de datos de RDS \[RDS.25\] deben usar un nombre de usuario de administrador personalizado](#)
- [Las instancias de base de datos de RDS \[RDS.26\] deben protegerse mediante un plan de copias de seguridad](#)
- [\[RDS.28\] Los clústeres de base de datos de RDS deben etiquetarse](#)
- [\[RDS.29\] Las instantáneas del clúster de base de datos de RDS deben etiquetarse](#)
- [\[RDS.30\] Las instancias de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.32\] Las instantáneas de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.33\] Los grupos de subredes de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.34\] Los clústeres de bases de datos Aurora MySQL deberían publicar los registros de auditoría en Logs CloudWatch](#)

- [Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[RDS.42\] Las instancias de base de datos de RDS para MariaDB deberían publicar registros en Logs CloudWatch](#)
- [\[RDS.44\] El RDS para las instancias de base de datos MariaDB debe cifrarse en tránsito](#)
- [Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo](#)
- [\[Redshift.14\] Los grupos de subredes del clúster de Redshift deben etiquetarse](#)
- [\[Redshift.15\] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos](#)
- [\[Redshift.17\] Los grupos de parámetros del clúster de Redshift deben estar etiquetados](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[RedshiftServerless.3\] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.4\] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1](#)
- [\[SageMaker.5\] SageMaker los modelos deberían bloquear el tráfico entrante](#)
- [\[SageMaker.6\] Las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas](#)
- [\[SageMaker.7\] SageMaker las imágenes deben estar etiquetadas](#)
- [\[ServiceCatalog.1\] Las carteras de Service Catalog solo deben compartirse dentro de una AWS organización](#)
- [\[SSM.5\] Los documentos SSM deben estar etiquetados](#)
- [\[StepFunctions.2\] Las actividades de Step Functions deben estar etiquetadas](#)

- [\[Transfer.2\] Los servidores de Transfer Family no deben utilizar el protocolo FTP para la conexión del punto de conexión](#)
- [\[Transfer.4\] Los acuerdos Transfer Family deben estar etiquetados](#)
- [\[Transfer.5\] Los certificados de Transfer Family deben estar etiquetados](#)
- [\[Transfer.6\] Los conectores Transfer Family deben estar etiquetados](#)
- [\[Transfer.7\] Los perfiles de Transfer Family deben estar etiquetados](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

Europa (Fráncfort)

Los siguientes controles no son compatibles en la región de Europa (Fráncfort).

- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)

- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

Europa (Irlanda)

Los siguientes controles no se admiten en la región Europa (Irlanda).

- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront5\] CloudFront las distribuciones deben tener el registro habilitado](#)

- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

Europa (Londres)

Los siguientes controles no son compatibles en la región de Europa (Londres).

- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)

- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[EC2.224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IoT Site Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Site Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)

- [\[Io TTwin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[Io TTwin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[Io TWireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

Europa (Milán)

Los siguientes controles no son compatibles en la región de Europa (Milán).

- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)

- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.4\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.8\] EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancias IMDSv2](#)
- [\[EC2.14\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 o :::/0 al puerto 3389](#)
- [\[EC2.24\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)

- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.177\] las sesiones espejo EC2 de tráfico deberían estar etiquetadas](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[ELB.2\] Los equilibradores de carga clásicos con agentes de escucha SSL/HTTPS deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [Los perfiles de AWS IoT Device Defender seguridad \[IoT.1\] deben estar etiquetados](#)
- [\[IoT.2\] las acciones de AWS IoT Core mitigación deben estar etiquetadas](#)
- [AWS IoT Core Las dimensiones de \[IoT.3\] deben estar etiquetadas](#)
- [Los AWS IoT Core autorizadores \[IoT.4\] deben estar etiquetados](#)
- [Los alias de los AWS IoT Core roles \[IoT.5\] deben estar etiquetados](#)
- [AWS IoT Core Las políticas \[IoT.6\] deben estar etiquetadas](#)
- [\[IoTEvents .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoTEvents .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoTEvents .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Site Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)

- [\[Io TSite Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[Io TSite Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[Io TSite Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[Io TSite Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[Io TTwin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[Io TWireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [\[Neptune.4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación](#)
- [\[Neptune.5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas](#)
- [\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM](#)
- [\[Neptune.8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas](#)
- [\[Neptune.9\] Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad](#)

- [\[RDS.1\] La instantánea de RDS debe ser privada](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[RedshiftServerless.3\] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público](#)
- [\[RedshiftServerless.4\] Los espacios de nombres de Redshift Serverless deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado](#)
- [\[RedshiftServerless.6\] Los espacios de nombres de Redshift Serverless deberían exportar los registros a los registros CloudWatch](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de base de datos predeterminado](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SSM.2\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de parche de COMPLIANT después de la instalación de un parche](#)
- [\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)

- [\[WorkSpaces.2\]](#) los volúmenes WorkSpaces raíz deben cifrarse en reposo

Europa (París)

Los siguientes controles no son compatibles en la región de Europa (París).

- [\[AppSync.1\]](#) Las cachés de las AWS AppSync API deben cifrarse en reposo
- [\[AppSync.6\]](#) Las cachés de las AWS AppSync API deben cifrarse en tránsito
- [\[CloudFront.1\]](#) CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado
- [\[CloudFront.3\]](#) CloudFront las distribuciones deben requerir el cifrado en tránsito
- [\[CloudFront.4\]](#) CloudFront Las distribuciones deben tener configurada la conmutación por error de origen
- [\[CloudFront.5\]](#) CloudFront las distribuciones deben tener el registro habilitado
- [\[CloudFront.6\]](#) CloudFront Las distribuciones deben tener WAF habilitado
- [\[CloudFront.7\]](#) CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados
- [\[CloudFront.8\]](#) CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS
- [\[CloudFront.9\]](#) CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados
- [\[CloudFront.10\]](#) CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados
- [\[CloudFront.12\]](#) CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes
- [\[CloudFront.13\]](#) CloudFront Las distribuciones deben usar el control de acceso de origen
- [\[CloudFront.14\]](#) CloudFront Las distribuciones deben etiquetarse
- [\[CodeGuruProfiler.1\]](#) Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados
- [\[CodeGuruReviewer.1\]](#) Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas
- [\[Connect.1\]](#) Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados
- [\[Connect.2\]](#) Las instancias de Amazon Connect deben tener el CloudWatch registro activado
- [\[EC2.224\]](#) No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon
- [\[EC2.173\]](#) Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos

- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FSx.5\] FSx para Windows, los sistemas de archivos del servidor de archivos deben configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[IoTEvents .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoTEvents .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoTEvents .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoTSiteWise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoTSiteWise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[IoTThingMaker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoTThingMaker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoTThingMaker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoTThingMaker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoTWireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoTWireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[IoTWireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)

- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

Europa (España)

Los siguientes controles no se admiten en la región Europa (España).

- [\[Account.2\] Cuentas de AWS debe formar parte de una organización AWS Organizations](#)
- [\[APIGateway.8\] Las rutas de API Gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas V2 de API Gateway](#)
- [\[Amplify.1\] Las aplicaciones de Amplify deben estar etiquetadas](#)
- [\[Amplify.2\] Las ramas de Amplify deben estar etiquetadas](#)
- [\[AppConfig.1\] AWS AppConfig las aplicaciones deben estar etiquetadas](#)
- [\[AppConfig.2\] los perfiles de AWS AppConfig configuración deben estar etiquetados](#)
- [\[AppConfig.3\] AWS AppConfig los entornos deben estar etiquetados](#)
- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[Backup.1\] Los puntos AWS Backup de recuperación deben cifrarse en reposo](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)

- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Cognito.1\] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.2\] Los certificados DMS deben estar etiquetados](#)
- [\[DMS.3\] Las suscripciones a eventos de DMS deben estar etiquetadas](#)
- [\[DMS.4\] Las instancias de replicación de DMS deben etiquetarse](#)
- [\[DMS.5\] Los grupos de subredes de replicación del DMS deben estar etiquetados](#)
- [\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)

- [\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)
- [\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado](#)
- [\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DocumentDb.6\] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.1\] Las instantáneas de Amazon EBS no se deben poder restaurar públicamente](#)
- [\[EC24\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.8\] EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancias IMDSv2](#)
- [\[EC2.14\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 o :::/0 al puerto 3389](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)
- [\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.25\] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red](#)

- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad](#)
- [\[EC2.34\] Las tablas de enrutamiento de las puertas de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.40\] Las puertas de enlace de EC2 NAT deben etiquetarse](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben etiquetarse](#)
- [\[EC251\] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.170\] Las plantillas de EC2 lanzamiento deben usar el servicio de metadatos de instancias versión 2 \(\) IMDSv2](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.175\] Las plantillas de EC2 lanzamiento deben estar etiquetadas](#)
- [\[EC2.177\] las sesiones espejo EC2 de tráfico deberían estar etiquetadas](#)
- [\[EC2.179\] Los objetivos EC2 de tráfico reflejados deben estar etiquetados](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] Los volúmenes de Amazon EFS deben estar en los planes de respaldo](#)
- [\[ELB.2\] Los equilibradores de carga clásicos con agentes de escucha SSL/HTTPS deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.14\] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.17\] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)
- [\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)

- [\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)
- [\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)
- [\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)
- [\[ES.4\] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[Glue.4\] Los trabajos de AWS Glue Spark deberían ejecutarse en versiones compatibles de AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[GuardDuty.3\] GuardDuty IPSets debe estar etiquetado](#)
- [\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)
- [\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)
- [\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)
- [\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)
- [\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)
- [\[IAM.19\] MFA se debe habilitar para todos los usuarios de IAM](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)

- [\[IAM.22\] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días](#)
- [\[IAM.24\] Los roles de IAM deben etiquetarse](#)
- [\[IAM.25\] Los usuarios de IAM deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IAM.27\] Las identidades de IAM no deben tener adjunta la política AWSCloud ShellFullAccess](#)
- [\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.2\] El análisis de ECR en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.4\] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado](#)
- [Los perfiles de AWS IoT Device Defender seguridad \[IoT.1\] deben estar etiquetados](#)
- [\[IoT.2\] las acciones de AWS IoT Core mitigación deben estar etiquetadas](#)
- [AWS IoT Core Las dimensiones de \[IoT.3\] deben estar etiquetadas](#)
- [Los AWS IoT Core autorizadores \[IoT.4\] deben estar etiquetados](#)
- [Los alias de los AWS IoT Core roles \[IoT.5\] deben estar etiquetados](#)
- [AWS IoT Core Las políticas \[IoT.6\] deben estar etiquetadas](#)
- [\[IoT Events .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoT Events .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Events .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Site Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Site Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[IoT TTwin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoT TTwin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoT TTwin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoT TTwin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoT Wireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)

- [\[Io Wireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)
- [\[KMS.1\] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.2\] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS](#)
- [\[Lambda.1\] Las políticas de función de Lambda deberían prohibir el acceso público](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)
- [\[MQ.2\] Los corredores de ActiveMQ deberían transmitir los registros de auditoría a CloudWatch](#)
- [\[MQ.3\] Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[MQ.4\] Los agentes de Amazon MQ deben estar etiquetados](#)
- [\[MQ.5\] Los corredores ActiveMQ deben usar el modo de implementación activo/en espera](#)
- [\[MQ.6\] Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [\[Neptune.4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación](#)
- [\[Neptune.5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas](#)
- [\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM](#)
- [\[Neptune.8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas](#)

- [\[Neptune.9\] Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad](#)
- [Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)
- [Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)
- [Los OpenSearch dominios \[Opensearch.3\] deben cifrar los datos enviados entre nodos](#)
- [El registro de errores de OpenSearch dominio \[Opensearch.4\] en CloudWatch Logs debe estar activado](#)
- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)
- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los OpenSearch dominios \[Opensearch.7\] deben tener habilitado un control de acceso detallado](#)
- [\[Opensearch.8\] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente](#)
- [Los OpenSearch dominios \[Opensearch.9\] deben estar etiquetados](#)
- [Los OpenSearch dominios \[Opensearch.10\] deben tener instalada la última actualización de software](#)
- [Los OpenSearch dominios \[Opensearch.11\] deben tener al menos tres nodos principales dedicados](#)
- [\[RDS.1\] La instantánea de RDS debe ser privada](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [Los clústeres de bases de datos de RDS \[RDS.15\] deben configurarse para varias zonas de disponibilidad](#)
- [Las instancias de base de datos de RDS \[RDS.26\] deben protegerse mediante un plan de copias de seguridad](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[RDS.37\] Los clústeres de bases de datos Aurora PostgreSQL deberían publicar registros en Logs CloudWatch](#)
- [Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)

- [\[S3.6\] Las políticas de compartimentos de uso general de S3 deberían restringir el acceso a otros Cuentas de AWS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] las instancias de SageMaker notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook](#)
- [\[SageMaker.5\] SageMaker los modelos deberían bloquear el tráfico entrante](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SQS.3\] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público](#)
- [\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [\[Transfer.3\] Los conectores Transfer Family deben tener habilitado el registro](#)
- [\[Transfer.4\] Los acuerdos Transfer Family deben estar etiquetados](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [La AWS WAF web de \[WAF.10\] ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

Europa (Estocolmo)

Los siguientes controles no son compatibles en la región de Europa (Estocolmo).

- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)

- [\[DocumentDb.6\]](#) Los clústeres de Amazon DocumentDB deben cifrarse en tránsito
- [\[DynamoDB.3\]](#) Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- [\[DynamoDB.7\]](#) Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito
- [\[EC2.224\]](#) No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon
- [\[EC2.173\]](#) Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos
- [\[ECR.4\]](#) Los repositorios públicos de ECR deben estar etiquetados
- [\[FraudDetector.1\]](#) Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados
- [\[FraudDetector.2\]](#) Las etiquetas de Amazon Fraud Detector deben estar etiquetadas
- [\[FraudDetector.3\]](#) Los resultados de Amazon Fraud Detector deben estar etiquetados
- [\[FraudDetector.4\]](#) Las variables de Amazon Fraud Detector deben estar etiquetadas
- [\[GlobalAccelerator.1\]](#) Los aceleradores de Global Accelerator deben estar etiquetados
- [\[IAM.26\]](#) Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse
- [\[IoTEvents.1\]](#) Las entradas de AWS IoT Events deben estar etiquetadas
- [\[IoTEvents.2\]](#) Los modelos de detectores de AWS IoT Events deben estar etiquetados
- [\[IoTEvents.3\]](#) Los modelos de alarma de AWS IoT Events deben estar etiquetados
- [\[IoTSiteWise.1\]](#) Los modelos de SiteWise activos de AWS IoT deben estar etiquetados
- [\[IoTSiteWise.2\]](#) SiteWise Los paneles de AWS IoT deben estar etiquetados
- [\[IoTSiteWise.3\]](#) SiteWise Las pasarelas de AWS IoT deben estar etiquetadas
- [\[IoTSiteWise.4\]](#) Los SiteWise portales de AWS IoT deben estar etiquetados
- [\[IoTSiteWise.5\]](#) Los SiteWise proyectos de AWS IoT deben estar etiquetados
- [\[IoTThingMaker.1\]](#) Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados
- [\[IoTThingMaker.2\]](#) Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados
- [\[IoTThingMaker.3\]](#) TwinMaker Las escenas de AWS IoT deben estar etiquetadas
- [\[IoTThingMaker.4\]](#) TwinMaker Las entidades de AWS IoT deben estar etiquetadas
- [\[IoTWireless.1\]](#) Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados
- [\[IoTWireless.2\]](#) Los perfiles del servicio AWS IoT Wireless deben estar etiquetados
- [\[IoTWireless.3\]](#) Las tareas de AWS IoT FUOTA deben estar etiquetadas
- [\[IVS.1\]](#) Los pares de teclas de reproducción del IVS deben estar etiquetados
- [\[IVS.2\]](#) Las configuraciones de grabación del IVS deben estar etiquetadas

- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

Europa (Zúrich)

Los siguientes controles no son compatibles en la región de Europa (Zúrich).

- [\[APIGateway.8\] Las rutas de API Gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas V2 de API Gateway](#)
- [\[Amplify.1\] Las aplicaciones de Amplify deben estar etiquetadas](#)
- [\[Amplify.2\] Las ramas de Amplify deben estar etiquetadas](#)
- [\[AppConfig.1\] AWS AppConfig las aplicaciones deben estar etiquetadas](#)
- [\[AppConfig.2\] los perfiles de AWS AppConfig configuración deben estar etiquetados](#)
- [\[AppConfig.3\] AWS AppConfig los entornos deben estar etiquetados](#)
- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)

- [\[Backup.1\] Los puntos AWS Backup de recuperación deben cifrarse en reposo](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CloudTrail.6\] Asegurar que los CloudTrail registros del bucket de S3 no son de acceso público](#)
- [\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el bucket de CloudTrail S3](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Cognito.1\] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.2\] Los certificados DMS deben estar etiquetados](#)

- [\[DMS.3\] Las suscripciones a eventos de DMS deben estar etiquetadas](#)
- [\[DMS.4\] Las instancias de replicación de DMS deben etiquetarse](#)
- [\[DMS.5\] Los grupos de subredes de replicación del DMS deben estar etiquetados](#)
- [\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)
- [\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado](#)
- [\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DocumentDb.6\] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC24\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.8\] EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancias IMDSv2](#)

- [\[EC2.14\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0.0.0/0 o: :/0 al puerto 3389](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)
- [\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.25\] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red](#)
- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.170\] Las plantillas de EC2 lanzamiento deben usar el servicio de metadatos de instancias versión 2 \(\) IMDSv2](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.175\] Las plantillas de EC2 lanzamiento deben estar etiquetadas](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] Los volúmenes de Amazon EFS deben estar en los planes de respaldo](#)
- [\[ELB.2\] Los equilibradores de carga clásicos con agentes de escucha SSL/HTTPS deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.14\] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.17\] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)
- [\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)
- [\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)

- [\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)
- [\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)
- [\[ES.4\] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[Glue.4\] Los trabajos de AWS Glue Spark deberían ejecutarse en versiones compatibles de AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[GuardDuty.3\] GuardDuty IPSets debe estar etiquetado](#)
- [\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)
- [\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)
- [\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)
- [\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)
- [\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)
- [\[IAM.19\] MFA se debe habilitar para todos los usuarios de IAM](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)
- [\[IAM.22\] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días](#)
- [\[IAM.24\] Los roles de IAM deben etiquetarse](#)

- [\[IAM.25\] Los usuarios de IAM deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IAM.27\] Las identidades de IAM no deben tener adjunta la política AWS Cloud Shell Full Access](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [Los perfiles de AWS IoT Device Defender seguridad \[IoT.1\] deben estar etiquetados](#)
- [\[IoT.2\] las acciones de AWS IoT Core mitigación deben estar etiquetadas](#)
- [AWS IoT Core Las dimensiones de \[IoT.3\] deben estar etiquetadas](#)
- [Los AWS IoT Core autorizadores \[IoT.4\] deben estar etiquetados](#)
- [Los alias de los AWS IoT Core roles \[IoT.5\] deben estar etiquetados](#)
- [AWS IoT Core Las políticas \[IoT.6\] deben estar etiquetadas](#)
- [\[IoT Events .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoT Events .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Events .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Site Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Site Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Twin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoT Wireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)
- [\[KMS.1\] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS](#)

- [\[KMS.2\] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)
- [\[MQ.2\] Los corredores de ActiveMQ deberían transmitir los registros de auditoría a CloudWatch](#)
- [\[MQ.3\] Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[MQ.4\] Los agentes de Amazon MQ deben estar etiquetados](#)
- [\[MQ.5\] Los corredores ActiveMQ deben usar el modo de implementación activo/en espera](#)
- [\[MQ.6\] Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [\[Neptune.4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación](#)
- [\[Neptune.5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas](#)
- [\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM](#)
- [\[Neptune.8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas](#)
- [\[Neptune.9\] Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad](#)
- [Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)
- [Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)
- [Los OpenSearch dominios \[Opensearch.3\] deben cifrar los datos enviados entre nodos](#)
- [El registro de errores de OpenSearch dominio \[Opensearch.4\] en CloudWatch Logs debe estar activado](#)
- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)

- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los OpenSearch dominios \[Opensearch.7\] deben tener habilitado un control de acceso detallado](#)
- [\[Opensearch.8\] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente](#)
- [Los OpenSearch dominios \[Opensearch.9\] deben estar etiquetados](#)
- [Los OpenSearch dominios \[Opensearch.10\] deben tener instalada la última actualización de software](#)
- [Los OpenSearch dominios \[Opensearch.11\] deben tener al menos tres nodos principales dedicados](#)
- [\[RDS.1\] La instantánea de RDS debe ser privada](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [Las instancias de base de datos de RDS \[RDS.26\] deben protegerse mediante un plan de copias de seguridad](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] las instancias de SageMaker notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook](#)
- [\[SageMaker.5\] SageMaker los modelos deberían bloquear el tráfico entrante](#)
- [\[SageMaker.6\] Las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas](#)
- [\[SageMaker.7\] SageMaker las imágenes deben estar etiquetadas](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)

- [\[SQS.1\] Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SQS.3\] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público](#)
- [\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [\[Transfer.3\] Los conectores Transfer Family deben tener habilitado el registro](#)
- [\[Transfer.4\] Los acuerdos Transfer Family deben estar etiquetados](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [La AWS WAF web de \[WAF.10\] ACLs debe tener al menos una regla o grupo de reglas](#)
- [El registro de ACL AWS WAF web de \[WAF.11\] debe estar habilitado](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

Israel (Tel Aviv)

Los siguientes controles no se admiten en la región de Israel (Tel Aviv).

- [\[APIGateway.8\] Las rutas de API Gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas V2 de API Gateway](#)
- [\[Amplify.1\] Las aplicaciones de Amplify deben estar etiquetadas](#)
- [\[Amplify.2\] Las ramas de Amplify deben estar etiquetadas](#)
- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.2\] AWS AppSync debe tener habilitado el registro a nivel de campo](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves de API](#)

- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[Backup.1\] Los puntos AWS Backup de recuperación deben cifrarse en reposo](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[Batch.1\] Las colas de trabajos por lotes deben estar etiquetadas](#)
- [\[Batch.3\] Los entornos de procesamiento por lotes deben etiquetarse](#)
- [\[Batch.4\] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[DMS.2\] Los certificados DMS deben estar etiquetados](#)

- [\[DMS.3\] Las suscripciones a eventos de DMS deben estar etiquetadas](#)
- [\[DMS.4\] Las instancias de replicación de DMS deben etiquetarse](#)
- [\[DMS.5\] Los grupos de subredes de replicación del DMS deben estar etiquetados](#)
- [\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)
- [\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado](#)
- [\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DocumentDb.6\] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC24\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.14\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0/0 o :/0 al puerto 3389](#)

- [\[EC220\] Ambos túneles de VPN de una conexión de AWS Site-to-Site VPN deben estar activos](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.25\] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red](#)
- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad](#)
- [\[EC2.33\] Las conexiones de puerta de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.34\] Las tablas de enrutamiento de las puertas de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.40\] Las puertas de enlace de EC2 NAT deben etiquetarse](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben etiquetarse](#)
- [\[EC251\] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)
- [\[EC2.55\] VPCs debe configurarse con un punto final de interfaz para la API ECR](#)
- [\[EC2.56\] VPCs debe configurarse con un punto final de interfaz para Docker Registry](#)
- [\[EC2.57\] VPCs debe configurarse con un punto final de interfaz para Systems Manager](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.170\] Las plantillas de EC2 lanzamiento deben usar el servicio de metadatos de instancias versión 2 \(\) IMDSv2](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.175\] Las plantillas de EC2 lanzamiento deben estar etiquetadas](#)
- [\[EC2.177\] las sesiones espejo EC2 de tráfico deberían estar etiquetadas](#)
- [\[EC2.179\] Los objetivos EC2 de tráfico reflejados deben estar etiquetados](#)
- [\[ECR.2\] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas](#)
- [\[ECR.3\] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)

- [\[ECR.5\] Los repositorios de ECR deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [\[ECS.16\] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] Los volúmenes de Amazon EFS deben estar en los planes de respaldo](#)
- [\[EFS.3\] Los puntos de acceso EFS deben aplicar un directorio raíz](#)
- [\[EFS.4\] Los puntos de acceso EFS deben imponer una identidad de usuario](#)
- [\[EFS.8\] Los sistemas de archivos de EFS deben cifrarse en reposo](#)
- [\[EKS.2\] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible](#)
- [\[EKS.6\] Los clústeres de EKS deben etiquetarse](#)
- [\[EKS.7\] Las configuraciones de los proveedores de identidad de EKS deben etiquetarse](#)
- [\[EKS.8\] Los clústeres de EKS deben tener habilitado el registro de auditoría](#)
- [\[ELB.2\] Los equilibradores de carga clásicos con agentes de escucha SSL/HTTPS deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.14\] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.17\] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.2\] ElastiCache Los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias](#)
- [\[ElastiCache.3\] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática](#)
- [\[ElastiCache.4\] los grupos de ElastiCache replicación deben estar cifrados en reposo](#)
- [\[ElastiCache.5\] los grupos de ElastiCache replicación deben cifrarse en tránsito](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)
- [\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)
- [\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)

- [\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)
- [\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)
- [\[EMR.3\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo](#)
- [\[ES.4\] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[Glue.4\] Los trabajos de AWS Glue Spark deberían ejecutarse en versiones compatibles de AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[GuardDuty.3\] GuardDuty IPSets debe estar etiquetado](#)
- [\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)
- [\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)
- [\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)
- [\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)
- [\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)
- [\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)
- [\[IAM.7\] Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)
- [\[IAM.10\] Las políticas de contraseñas de usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.11\] Asegurar que la política de contraseñas de IAM requiera al menos una letra mayúscula](#)
- [\[IAM.12\] Asegurar que la política de contraseñas de IAM requiera al menos una letra minúscula](#)

- [\[IAM.13\] Asegurar que la política de contraseñas de IAM requiera al menos un símbolo](#)
- [\[IAM.14\] Asegurar que la política de contraseñas de IAM requiera al menos un número](#)
- [\[IAM.15\] Asegurar que la política de contraseñas de IAM requiera una longitud mínima de 14 o más](#)
- [\[IAM.16\] Asegurar que la política de contraseñas de IAM impida la reutilización de contraseñas](#)
- [\[IAM.17\] Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos](#)
- [\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)
- [\[IAM.19\] MFA se debe habilitar para todos los usuarios de IAM](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)
- [\[IAM.22\] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días](#)
- [\[IAM.24\] Los roles de IAM deben etiquetarse](#)
- [\[IAM.25\] Los usuarios de IAM deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IAM.27\] Las identidades de IAM no deben tener adjunta la política AWS Cloud Shell Full Access](#)
- [\[IAM.28\] El analizador de acceso externo del Analizador de acceso de IAM debe habilitarse](#)
- [\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.2\] El análisis de ECR en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.4\] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado](#)
- [Los perfiles de AWS IoT Device Defender seguridad \[IoT.1\] deben estar etiquetados](#)
- [\[IoT.2\] las acciones de AWS IoT Core mitigación deben estar etiquetadas](#)
- [AWS IoT Core Las dimensiones de \[IoT.3\] deben estar etiquetadas](#)
- [Los AWS IoT Core autorizadores \[IoT.4\] deben estar etiquetados](#)
- [Los alias de los AWS IoT Core roles \[IoT.5\] deben estar etiquetados](#)
- [AWS IoT Core Las políticas \[IoT.6\] deben estar etiquetadas](#)
- [\[IoT Events .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoT Events .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)

- [\[Io TEvents .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[Io TSite Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[Io TSite Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[Io TSite Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[Io TSite Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[Io TSite Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[Io TTwin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[Io TWireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)
- [\[Kinesis.1\] Las transmisiones de Kinesis deben cifrarse en reposo](#)
- [\[Kinesis.2\] Las transmisiones de Kinesis deben etiquetarse](#)
- [\[Kinesis.3\] Las transmisiones de Kinesis deben tener un periodo adecuado de retención de datos](#)
- [\[KMS.1\] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.2\] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS](#)
- [\[Lambda.5\] Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[MQ.2\] Los corredores de ActiveMQ deberían transmitir los registros de auditoría a CloudWatch](#)
- [\[MQ.3\] Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[MQ.4\] Los agentes de Amazon MQ deben estar etiquetados](#)
- [\[MQ.5\] Los corredores ActiveMQ deben usar el modo de implementación activo/en espera](#)

- [\[MQ.6\] Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres](#)
- [\[MSK.1\] Los clústeres de MSK deben cifrarse en tránsito entre los nodos intermediarios](#)
- [\[MSK.2\] Los clústeres de MSK deberían tener configurada una supervisión mejorada](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de cambio de subred](#)
- [Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)
- [Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)
- [Los OpenSearch dominios \[Opensearch.3\] deben cifrar los datos enviados entre nodos](#)
- [El registro de errores de OpenSearch dominio \[Opensearch.4\] en CloudWatch Logs debe estar activado](#)
- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)
- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los OpenSearch dominios \[Opensearch.7\] deben tener habilitado un control de acceso detallado](#)
- [\[Opensearch.8\] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente](#)
- [Los OpenSearch dominios \[Opensearch.9\] deben estar etiquetados](#)
- [Los OpenSearch dominios \[Opensearch.10\] deben tener instalada la última actualización de software](#)
- [Los OpenSearch dominios \[Opensearch.11\] deben tener al menos tres nodos principales dedicados](#)
- [\[RDS.1\] La instantánea de RDS debe ser privada](#)
- [Las instantáneas de clústeres y bases de datos de RDS \[RDS.4\] deben cifrarse cuando están inactivas](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [Los clústeres de bases de datos de RDS \[RDS.15\] deben configurarse para varias zonas de disponibilidad](#)
- [Las instancias de base de datos de RDS \[RDS.26\] deben protegerse mediante un plan de copias de seguridad](#)

- [\[RDS.29\] Las instantáneas del clúster de base de datos de RDS deben etiquetarse](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[RDS.37\] Los clústeres de bases de datos Aurora PostgreSQL deberían publicar registros en Logs CloudWatch](#)
- [Los clústeres de Amazon Redshift \[Redshift.3\] deben tener habilitadas las instantáneas automáticas](#)
- [Los clústeres de Amazon Redshift \[Redshift.8\] no deben usar el nombre de usuario de administrador predeterminado](#)
- [Los clústeres de Redshift \[Redshift.9\] no deben usar el nombre de base de datos predeterminado](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] las instancias de SageMaker notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook](#)
- [\[SageMaker.5\] SageMaker los modelos deberían bloquear el tráfico entrante](#)
- [\[ServiceCatalog.1\] Las carteras de Service Catalog solo deben compartirse dentro de una AWS organización](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SQS.3\] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público](#)
- [\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)

- [\[SSM.4\] Los documentos SSM no deben ser públicos](#)
- [\[StepFunctions.1\] Las máquinas de estado de Step Functions deberían tener el registro activado](#)
- [\[Transfer.3\] Los conectores Transfer Family deben tener habilitado el registro](#)
- [\[Transfer.4\] Los acuerdos Transfer Family deben estar etiquetados](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [El registro de ACL AWS WAF web de \[WAF.11\] debe estar habilitado](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

México (central)

Los siguientes controles no se admiten en la región México (centro).

- [\[ACM.1\] Los certificados importados y emitidos por ACM deben renovarse después de un período de tiempo específico](#)
- [\[ACM.2\] Los certificados RSA administrados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)
- [\[ACM.3\] Los certificados ACM deben estar etiquetados](#)
- [\[Cuenta.1\] La información de contacto de seguridad debe proporcionarse para un Cuenta de AWS](#)
- [\[Account.2\] Cuentas de AWS debe formar parte de una organización AWS Organizations](#)
- [\[APIGateway.1\] El registro de ejecución de WebSocket REST y API de API Gateway debe estar habilitado](#)
- [\[APIGateway.2\] Las etapas de la API de REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend](#)
- [\[APIGateway.3\] Las etapas de la API de REST de API Gateway tener AWS X-Ray habilitado el rastreo](#)
- [\[APIGateway.4\] La API Gateway debe estar asociada a una ACL web de WAF](#)

- [\[APIGateway.5\] Los datos de la caché de la API de REST de API Gateway deben cifrarse en reposo](#)
- [\[APIGateway.8\] Las rutas de API Gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas V2 de API Gateway](#)
- [\[Amplify.1\] Las aplicaciones de Amplify deben estar etiquetadas](#)
- [\[Amplify.2\] Las ramas de Amplify deben estar etiquetadas](#)
- [\[AppConfig.1\] AWS AppConfig las aplicaciones deben estar etiquetadas](#)
- [\[AppConfig.2\] los perfiles de AWS AppConfig configuración deben estar etiquetados](#)
- [\[AppConfig.3\] AWS AppConfig los entornos deben estar etiquetados](#)
- [\[AppConfig.4\] Las asociaciones AWS AppConfig de extensiones deben estar etiquetadas](#)
- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.2\] AWS AppSync debe tener habilitado el registro a nivel de campo](#)
- [\[AppSync.4\] AWS AppSync APIs GraphQL debe estar etiquetado](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves de API](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[Athena.2\] Los catálogos de datos de Athena deben estar etiquetados](#)
- [\[Athena.3\] Los grupos de trabajo de Athena deben estar etiquetados](#)
- [\[Athena.4\] Los grupos de trabajo de Athena deben tener el registro habilitado](#)
- [\[AutoScaling.2\] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad](#)
- [\[AutoScaling.3\] Las configuraciones de lanzamiento de grupos de Auto Scaling deberían configurar las EC2 instancias para que requieran la versión 2 del Servicio de Metadatos de Instancia \(IMDSv2\)](#)
- [\[AutoScaling.6\] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad](#)
- [\[AutoScaling.9\] Los grupos de Amazon EC2 Auto Scaling deberían usar las plantillas de EC2 lanzamiento de Amazon](#)
- [\[AutoScaling.10\] Los grupos EC2 de Auto Scaling deben estar etiquetados](#)
- [\[Backup.1\] Los puntos AWS Backup de recuperación deben cifrarse en reposo](#)

- [\[Backup.2\] Los puntos AWS Backup de recuperación deben estar etiquetados](#)
- [\[Backup.3\] las AWS Backup bóvedas deben estar etiquetadas](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[Backup.5\] los planes de AWS Backup respaldo deben estar etiquetados](#)
- [\[Batch.1\] Las colas de trabajos por lotes deben estar etiquetadas](#)
- [\[Batch.2\] Las políticas de programación de lotes deben estar etiquetadas](#)
- [\[Batch.3\] Los entornos de procesamiento por lotes deben etiquetarse](#)
- [\[Batch.4\] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben etiquetarse](#)
- [\[CloudFormation.2\] las CloudFormation pilas deben estar etiquetadas](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CloudTrail.6\] Asegurar que los CloudTrail registros del bucket de S3 no son de acceso público](#)
- [\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el bucket de CloudTrail S3](#)
- [\[CloudTrail.9\] los registros de CloudTrail seguimiento deben etiquetarse](#)
- [\[CloudTrail.10\] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el cliente AWS KMS keys](#)

- [\[CloudWatch.17\] las acciones CloudWatch de alarma deben estar activadas](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeBuild.1\] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales](#)
- [\[CodeBuild.2\] Las variables de entorno CodeBuild del proyecto no deben contener credenciales de texto claro](#)
- [\[CodeBuild.3\] Los registros de CodeBuild S3 deben estar cifrados](#)
- [\[CodeBuild.4\] Los entornos de los CodeBuild proyectos deben tener una duración de registro AWS Config](#)
- [\[CodeBuild.7\] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Cognito.1\] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[DataFirehose.1\] Los flujos de entrega de Firehose deben cifrarse en reposo](#)
- [\[DataSync.1\] DataSync las tareas deberían tener el registro activado](#)
- [\[DataSync.2\] DataSync las tareas deben estar etiquetadas](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)
- [\[DMS.2\] Los certificados DMS deben estar etiquetados](#)
- [\[DMS.3\] Las suscripciones a eventos de DMS deben estar etiquetadas](#)
- [\[DMS.4\] Las instancias de replicación de DMS deben etiquetarse](#)
- [\[DMS.5\] Los grupos de subredes de replicación del DMS deben estar etiquetados](#)
- [\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)

- [\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)
- [\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado](#)
- [\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DocumentDb.6\] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.5\] Las tablas de DynamoDB deben etiquetarse](#)
- [\[DynamoDB.6\] Las tablas de DynamoDB deben tener la protección contra eliminación habilitada](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC24\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.21\] La red no ACLs debe permitir la entrada desde 0.0.0/0 al puerto 22 o al puerto 3389](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.25\] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red](#)

- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad](#)
- [\[EC2.33\] Las conexiones de puerta de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.34\] Las tablas de enrutamiento de las puertas de enlace de EC2 tránsito deben etiquetarse](#)
- [\[EC2.35\] Las interfaces EC2 de red deben etiquetarse](#)
- [\[EC2.36\] Las pasarelas de EC2 clientes deben estar etiquetadas](#)
- [\[EC2.37\] Las direcciones IP EC2 elásticas deben etiquetarse](#)
- [\[EC2.38\] EC2 las instancias deben estar etiquetadas](#)
- [\[EC2.39\] Las puertas de enlace de EC2 Internet deben etiquetarse](#)
- [\[EC2.40\] Las puertas de enlace de EC2 NAT deben etiquetarse](#)
- [La EC2 red \[EC2.41\] ACLs debe estar etiquetada](#)
- [\[EC2.42\] Las tablas de EC2 enrutamiento deben estar etiquetadas](#)
- [\[EC2.43\] los grupos EC2 de seguridad deben estar etiquetados](#)
- [EC2 Las subredes \[EC2.44\] deben estar etiquetadas](#)
- [\[EC2.45\] los EC2 volúmenes deben estar etiquetados](#)
- [\[EC2.46\] Amazon VPCs debería estar etiquetado](#)
- [\[EC2.47\] Los servicios de puntos de conexión de Amazon VPC deben etiquetarse](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben etiquetarse](#)
- [\[EC2.49\] Las conexiones de emparejamiento de Amazon VPC deben etiquetarse](#)
- [\[EC2.50\] Las puertas de enlace de EC2 VPN deben etiquetarse](#)
- [\[EC251\] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)
- [\[EC2.52\] Las EC2 puertas de enlace de](#)
- [\[EC2.53\] Los grupos EC2 de seguridad no deberían permitir la entrada de 0.0.0.0/0 a los puertos de administración de servidores remotos](#)
- [\[EC2.54\] Los grupos EC2 de seguridad no deberían permitir la entrada de: :/0 a los puertos de administración de servidores remotos](#)
- [\[EC2.55\] VPCs debe configurarse con un punto final de interfaz para la API ECR](#)
- [\[EC2.56\] VPCs debe configurarse con un punto final de interfaz para Docker Registry](#)
- [\[EC2.57\] VPCs debe configurarse con un punto final de interfaz para Systems Manager](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)

- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.170\] Las plantillas de EC2 lanzamiento deben usar el servicio de metadatos de instancias versión 2 \(\) IMDSv2](#)
- [\[EC2.171\] Las conexiones EC2 VPN deben tener el registro habilitado](#)
- [\[EC2.172\] La configuración del acceso público al bloqueo de EC2 VPC debería bloquear el tráfico de las puertas de enlace de Internet](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.174\] Los conjuntos de opciones de EC2 DHCP deben estar etiquetados](#)
- [\[EC2.175\] Las plantillas de EC2 lanzamiento deben estar etiquetadas](#)
- [\[EC2.176\] Las listas de EC2 prefijos deben estar etiquetadas](#)
- [\[EC2.177\] las sesiones espejo EC2 de tráfico deberían estar etiquetadas](#)
- [\[EC2.178\] Los filtros espejo de EC2 tráfico deben estar etiquetados](#)
- [\[EC2.179\] Los objetivos EC2 de tráfico reflejados deben estar etiquetados](#)
- [\[ECR.1\] Los repositorios privados del ECR deben tener configurado el escaneo de imágenes](#)
- [\[ECR.2\] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas](#)
- [\[ECR.3\] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[ECR.5\] Los repositorios de ECR deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [\[ECS.2\] Los servicios de ECS no deberían tener direcciones IP públicas asignadas automáticamente](#)
- [\[ECS.3\] Las definiciones de tareas de ECS no deben compartir el espacio de nombres de los procesos del anfitrión](#)
- [\[ECS.4\] Los contenedores de ECS deben ejecutarse sin privilegios](#)
- [\[ECS.5\] Los contenedores ECS deben limitarse al acceso de solo lectura a los sistemas de archivos raíz](#)
- [\[ECS.8\] Los secretos no deben pasarse como variables de entorno del contenedor](#)
- [\[ECS.9\] Las definiciones de tareas de ECS deben tener una configuración de registro](#)
- [\[ECS.10\] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate](#)
- [\[ECS.12\] Los clústeres de ECS deben usar Container Insights](#)

- [\[ECS.13\] Los servicios de ECS deben estar etiquetados](#)
- [\[ECS.14\] Los clústeres de ECS deben etiquetarse](#)
- [\[ECS.15\] Las definiciones de tareas de ECS deben etiquetarse](#)
- [\[ECS.16\] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas](#)
- [\[ECS.17\] Las definiciones de tareas de ECS no deben utilizar el modo de red host](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] Los volúmenes de Amazon EFS deben estar en los planes de respaldo](#)
- [\[EFS.3\] Los puntos de acceso EFS deben aplicar un directorio raíz](#)
- [\[EFS.4\] Los puntos de acceso EFS deben imponer una identidad de usuario](#)
- [\[EFS.5\] Los puntos de acceso de EFS deben etiquetarse](#)
- [\[EFS.6\] Los destinos de montaje de EFS no deben estar asociados a una subred pública](#)
- [\[EFS.7\] Los sistemas de archivos de EFS deben tener habilitadas las copias de seguridad automáticas](#)
- [\[EFS.8\] Los sistemas de archivos de EFS deben cifrarse en reposo](#)
- [\[EKS.2\] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible](#)
- [\[EKS.3\] Los clústeres de EKS deben usar secretos de Kubernetes cifrados](#)
- [\[EKS.6\] Los clústeres de EKS deben etiquetarse](#)
- [\[EKS.7\] Las configuraciones de los proveedores de identidad de EKS deben etiquetarse](#)
- [\[EKS.8\] Los clústeres de EKS deben tener habilitado el registro de auditoría](#)
- [\[ELB.7\] Los equilibradores de carga clásicos deberían tener habilitado el drenaje de conexiones](#)
- [\[ELB.10\] Equilibrador de carga clásico debe abarcar varias zonas de disponibilidad](#)
- [\[ELB.12\] Equilibrador de carga de aplicación debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.13\] Los equilibradores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad](#)
- [\[ELB.14\] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.17\] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas](#)

- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.2\] ElastiCache Los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias](#)
- [\[ElastiCache.3\] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática](#)
- [\[ElastiCache.4\] los grupos de ElastiCache replicación deben estar cifrados en reposo](#)
- [\[ElastiCache.5\] los grupos de ElastiCache replicación deben cifrarse en tránsito](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)
- [\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)
- [\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)
- [\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)
- [\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)
- [\[EMR.2\] La configuración de bloqueo del acceso público de Amazon EMR debe estar habilitada](#)
- [\[EMR.3\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo](#)
- [\[EMR.4\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito](#)
- [\[ES.3\] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos](#)
- [\[ES.4\] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros](#)
- [\[ES.5\] Los dominios de Elasticsearch deben tener habilitado el registro de auditoría](#)
- [\[ES.6\] Los dominios de Elasticsearch deben tener al menos tres nodos de datos](#)
- [\[ES.7\] Los dominios de Elasticsearch deben configurarse con al menos tres nodos maestros dedicados](#)
- [\[ES.8\] Las conexiones a dominios de Elasticsearch deben estar cifradas conforme a la política de seguridad TLS más reciente](#)
- [\[ES.9\] Los dominios de Elasticsearch deben estar etiquetados](#)
- [\[EventBridge.2\] los autobuses de EventBridge eventos deben estar etiquetados](#)

- [\[EventBridge.3\] Los autobuses de eventos EventBridge personalizados deben incluir una política basada en los recursos](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FSx.1\] en el caso FSx de OpenZFS, los sistemas de archivos deben configurarse para copiar etiquetas en copias de seguridad y volúmenes](#)
- [\[FSx.2\] FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad](#)
- [\[FSx.3\] FSx para los sistemas de archivos OpenZFS, debe configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[FSx.4\] FSx para los sistemas de archivos NetApp ONTAP, debe configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[FSx.5\] FSx para Windows, los sistemas de archivos del servidor de archivos deben configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[Glue.1\] los AWS Glue trabajos deben estar etiquetados](#)
- [\[Glue.3\] Las transformaciones AWS Glue de aprendizaje automático deben cifrarse en reposo](#)
- [\[Glue.4\] Los trabajos de AWS Glue Spark deberían ejecutarse en versiones compatibles de AWS Glue](#)
- [\[GuardDuty.1\] GuardDuty debería estar activado](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[GuardDuty.3\] GuardDuty IPSets debe estar etiquetado](#)
- [\[GuardDuty.4\] GuardDuty los detectores deben estar etiquetados](#)
- [\[GuardDuty.5\] La supervisión de registros de auditoría de GuardDuty EKS debe estar habilitada](#)
- [\[GuardDuty.6\] La protección de GuardDuty Lambda debe estar habilitada](#)
- [\[GuardDuty.7\] La supervisión en tiempo de ejecución de GuardDuty EKS debe estar habilitada](#)
- [\[GuardDuty.8\] La protección contra GuardDuty malware para EC2 debe estar habilitada](#)
- [\[GuardDuty.9\] La protección de GuardDuty RDS debe estar habilitada](#)

- [\[GuardDuty.10\] La protección de GuardDuty S3 debe estar habilitada](#)
- [\[GuardDuty.11\] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada](#)
- [\[GuardDuty.12\] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada](#)
- [\[GuardDuty.13\] La monitorización del GuardDuty EC2 tiempo de ejecución debe estar habilitada](#)
- [\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)
- [\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)
- [\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)
- [\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)
- [\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)
- [\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)
- [\[IAM.7\] Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)
- [\[IAM.10\] Las políticas de contraseñas de usuarios de IAM deben tener configuraciones seguras](#)
- [\[IAM.11\] Asegurar que la política de contraseñas de IAM requiera al menos una letra mayúscula](#)
- [\[IAM.12\] Asegurar que la política de contraseñas de IAM requiera al menos una letra minúscula](#)
- [\[IAM.13\] Asegurar que la política de contraseñas de IAM requiera al menos un símbolo](#)
- [\[IAM.14\] Asegurar que la política de contraseñas de IAM requiera al menos un número](#)
- [\[IAM.15\] Asegurar que la política de contraseñas de IAM requiera una longitud mínima de 14 o más](#)
- [\[IAM.16\] Asegurar que la política de contraseñas de IAM impida la reutilización de contraseñas](#)
- [\[IAM.17\] Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos](#)
- [\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)
- [\[IAM.19\] MFA se debe habilitar para todos los usuarios de IAM](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)
- [\[IAM.22\] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días](#)

- [\[IAM.23\] Los analizadores del Analizador de acceso de IAM deben etiquetarse](#)
- [\[IAM.24\] Los roles de IAM deben etiquetarse](#)
- [\[IAM.25\] Los usuarios de IAM deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IAM.27\] Las identidades de IAM no deben tener adjunta la política AWS Cloud Shell FullAccess](#)
- [\[IAM.28\] El analizador de acceso externo del Analizador de acceso de IAM debe habilitarse](#)
- [\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.2\] El análisis de ECR en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.4\] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado](#)
- [Los perfiles de AWS IoT Device Defender seguridad \[IoT.1\] deben estar etiquetados](#)
- [\[IoT.2\] las acciones de AWS IoT Core mitigación deben estar etiquetadas](#)
- [AWS IoT Core Las dimensiones de \[IoT.3\] deben estar etiquetadas](#)
- [Los AWS IoT Core autorizadores \[IoT.4\] deben estar etiquetados](#)
- [Los alias de los AWS IoT Core roles \[IoT.5\] deben estar etiquetados](#)
- [AWS IoT Core Las políticas \[IoT.6\] deben estar etiquetadas](#)
- [\[IoT Events .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoT Events .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Events .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Site Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Site Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Twin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoT Wireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)

- [\[IoT Wireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)
- [\[Kinesis.1\] Las transmisiones de Kinesis deben cifrarse en reposo](#)
- [\[Kinesis.2\] Las transmisiones de Kinesis deben etiquetarse](#)
- [\[Kinesis.3\] Las transmisiones de Kinesis deben tener un periodo adecuado de retención de datos](#)
- [\[KMS.1\] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.2\] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.3\] no AWS KMS keys debe eliminarse involuntariamente](#)
- [\[KMS.5\] Las claves KMS no deben ser de acceso público](#)
- [\[Lambda.5\] Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad](#)
- [\[Lambda.6\] Las funciones de Lambda deben estar etiquetadas](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)
- [\[MQ.2\] Los corredores de ActiveMQ deberían transmitir los registros de auditoría a CloudWatch](#)
- [\[MQ.3\] Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[MQ.4\] Los agentes de Amazon MQ deben estar etiquetados](#)
- [\[MQ.5\] Los corredores ActiveMQ deben usar el modo de implementación activo/en espera](#)
- [\[MQ.6\] Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres](#)
- [\[MSK.1\] Los clústeres de MSK deben cifrarse en tránsito entre los nodos intermediarios](#)
- [\[MSK.2\] Los clústeres de MSK deberían tener configurada una supervisión mejorada](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)

- [\[Neptune.4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación](#)
- [\[Neptune.5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas](#)
- [\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM](#)
- [\[Neptune.8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas](#)
- [\[Neptune.9\] Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad](#)
- [Los NetworkFirewall firewalls de Network Firewall se deben implementar en varias zonas de disponibilidad](#)
- [\[NetworkFirewall.2\] El registro de Network Firewall debe estar habilitado](#)
- [\[NetworkFirewall.3\] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas](#)
- [\[NetworkFirewall.4\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos](#)
- [\[NetworkFirewall.5\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados](#)
- [El grupo de reglas de Stateless Network Firewall \[NetworkFirewall.6\] no debe estar vacío](#)
- [Los NetworkFirewall firewalls de Network Firewall se deben etiquetar](#)
- [\[NetworkFirewall.8\] Las políticas de firewall de Network Firewall se deben etiquetar](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de eliminación](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de cambio de subred](#)
- [Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)
- [Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)
- [Los OpenSearch dominios \[Opensearch.3\] deben cifrar los datos enviados entre nodos](#)
- [El registro de errores de OpenSearch dominio \[Opensearch.4\] en CloudWatch Logs debe estar activado](#)

- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)
- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los OpenSearch dominios \[Opensearch.7\] deben tener habilitado un control de acceso detallado](#)
- [\[Opensearch.8\] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente](#)
- [Los OpenSearch dominios \[Opensearch.9\] deben estar etiquetados](#)
- [Los OpenSearch dominios \[Opensearch.10\] deben tener instalada la última actualización de software](#)
- [Los OpenSearch dominios \[Opensearch.11\] deben tener al menos tres nodos principales dedicados](#)
- [La autoridad emisora de certificados AWS Private CA raíz \[PCA.1\] debe estar deshabilitada](#)
- [\[PCA.2\] Se debe etiquetar a las autoridades certificadoras de CA AWS privadas](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [Los clústeres de bases de datos de RDS \[RDS.16\] deben configurarse para copiar etiquetas en las instantáneas](#)
- [Las instancias de base de datos de RDS \[RDS.17\] deben configurarse para copiar etiquetas en las instantáneas](#)
- [Las instancias de RDS \[RDS.18\] deben implementarse en una VPC](#)
- [Las suscripciones de notificación de eventos de RDS \[RDS.19\] existentes deben configurarse para los eventos de clúster críticos](#)
- [Las suscripciones de notificación de eventos de RDS \[RDS.20\] existentes deben configurarse para eventos críticos de instancias de bases de datos](#)
- [Se debe configurar una suscripción a las notificaciones de eventos de RDS \[RDS.21\] para los eventos críticos de los grupos de parámetros de bases de datos](#)
- [Se debe configurar una suscripción a las notificaciones de eventos de RDS \[RDS.22\] para los eventos críticos de los grupos de seguridad de bases de datos](#)
- [Las instancias RDS \[RDS.23\] no deben usar el puerto predeterminado de un motor de base de datos](#)
- [Los clústeres de bases de datos de RDS \[RDS.24\] deben usar un nombre de usuario de administrador personalizado](#)
- [Las instancias de bases de datos de RDS \[RDS.25\] deben usar un nombre de usuario de administrador personalizado](#)

- [Las instancias de base de datos de RDS \[RDS.26\] deben protegerse mediante un plan de copias de seguridad](#)
- [Los clústeres de bases de datos de RDS \[RDS.27\] deben cifrarse en reposo](#)
- [\[RDS.28\] Los clústeres de base de datos de RDS deben etiquetarse](#)
- [\[RDS.29\] Las instantáneas del clúster de base de datos de RDS deben etiquetarse](#)
- [\[RDS.30\] Las instancias de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.32\] Las instantáneas de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.33\] Los grupos de subredes de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.34\] Los clústeres de bases de datos Aurora MySQL deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[RDS.36\] Las instancias de base de datos de RDS para PostgreSQL deben publicar registros en Logs CloudWatch](#)
- [\[RDS.37\] Los clústeres de bases de datos Aurora PostgreSQL deberían publicar registros en Logs CloudWatch](#)
- [\[RDS.38\] Las instancias de base de datos de RDS para PostgreSQL deben cifrarse en tránsito](#)
- [\[RDS.39\] Las instancias de base de datos de RDS para MySQL deben cifrarse en tránsito](#)
- [\[RDS.40\] Las instancias de base de datos de RDS para SQL Server deberían publicar los registros en Logs CloudWatch](#)
- [\[RDS.41\] Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito](#)
- [\[RDS.42\] Las instancias de base de datos de RDS para MariaDB deberían publicar registros en Logs CloudWatch](#)
- [\[RDS.44\] El RDS para las instancias de base de datos MariaDB debe cifrarse en tránsito](#)
- [\[Redshift.1\] Los clústeres de Amazon Redshift deberían prohibir el acceso público](#)
- [Las conexiones a los clústeres de Amazon Redshift \[Redshift.2\] deben cifrarse en tránsito](#)
- [Los clústeres de Amazon Redshift \[Redshift.3\] deben tener habilitadas las instantáneas automáticas](#)
- [Los clústeres de Amazon Redshift \[Redshift.4\] deben tener habilitado el registro de auditoría](#)
- [Amazon Redshift \[Redshift.6\] debería tener habilitadas las actualizaciones automáticas a las versiones principales](#)

- [Los clústeres de Redshift \[Redshift.7\] deberían utilizar un enrutamiento de VPC mejorado](#)
- [Los clústeres de Amazon Redshift \[Redshift.8\] no deben usar el nombre de usuario de administrador predeterminado](#)
- [Los clústeres de Redshift \[Redshift.9\] no deben usar el nombre de base de datos predeterminado](#)
- [Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo](#)
- [\[Redshift.11\] Los clústeres de Redshift deben etiquetarse](#)
- [\[Redshift.12\] Las suscripciones a notificaciones de eventos de Redshift deben etiquetarse](#)
- [\[Redshift.13\] Las instantáneas del clúster de Redshift deben etiquetarse](#)
- [\[Redshift.14\] Los grupos de subredes del clúster de Redshift deben etiquetarse](#)
- [\[Redshift.15\] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos](#)
- [\[Redshift.16\] Los grupos de subredes de clústeres de Redshift deben tener subredes de varias zonas de disponibilidad](#)
- [\[Redshift.17\] Los grupos de parámetros del clúster de Redshift deben estar etiquetados](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[RedshiftServerless.3\] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público](#)
- [\[RedshiftServerless.4\] Los espacios de nombres de Redshift Serverless deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado](#)
- [\[RedshiftServerless.6\] Los espacios de nombres de Redshift Serverless deberían exportar los registros a los registros CloudWatch](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de base de datos predeterminado](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.7\] Los buckets de uso general de S3 deben usar la replicación entre regiones](#)

- [\[S3.10\] Los buckets de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida](#)
- [\[S3.11\] Los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos](#)
- [\[S3.12\] no ACLs debe usarse para administrar el acceso de los usuarios a los depósitos de uso general de S3](#)
- [\[S3.13\] Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida](#)
- [\[S3.19\] Los puntos de acceso de S3 deben tener habilitada la configuración de Bloqueo de acceso público](#)
- [\[S3.20\] Los buckets de uso general de S3 deben tener habilitada la eliminación de MFA](#)
- [\[S3.22\] Los buckets de uso general de S3 deben registrar eventos de escritura a nivel de objeto](#)
- [\[S3.23\] Los buckets de uso general de S3 deben registrar eventos de lectura a nivel de objeto](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] las instancias de SageMaker notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook](#)
- [\[SageMaker.4\] Las variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1](#)
- [\[SageMaker.5\] SageMaker los modelos deberían bloquear el tráfico entrante](#)
- [\[SageMaker.6\] Las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas](#)
- [\[SageMaker.7\] SageMaker las imágenes deben estar etiquetadas](#)
- [\[SageMaker.8\] las instancias de SageMaker notebook deberían ejecutarse en plataformas compatibles](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [\[SecretsManager.1\] Los secretos de Secrets Manager deberían tener habilitada la rotación automática](#)
- [\[SecretsManager.2\] Los secretos de Secrets Manager configurados con rotación automática deberían rotar correctamente](#)

- [\[SecretsManager.3\] Eliminar los secretos de Secrets Manager no utilizados](#)
- [\[SecretsManager.4\] Los secretos de Secrets Manager deben rotarse en un número específico de días](#)
- [\[SecretsManager.5\] Los secretos de Secrets Manager deben estar etiquetados](#)
- [\[ServiceCatalog.1\] Las carteras de Service Catalog solo deben compartirse dentro de una AWS organización](#)
- [\[SNS.3\] Los temas de SNS deben etiquetarse](#)
- [\[SNS.4\] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SQS.3\] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público](#)
- [\[SSM.3\] EC2 Las instancias Amazon administradas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [\[SSM.4\] Los documentos SSM no deben ser públicos](#)
- [\[SSM.5\] Los documentos SSM deben estar etiquetados](#)
- [\[StepFunctions.1\] Las máquinas de estado de Step Functions deberían tener el registro activado](#)
- [\[StepFunctions.2\] Las actividades de Step Functions deben estar etiquetadas](#)
- [Los AWS Transfer Family flujos de trabajo de \[Transfer.1\] deben estar etiquetados](#)
- [\[Transfer.2\] Los servidores de Transfer Family no deben utilizar el protocolo FTP para la conexión del punto de conexión](#)
- [\[Transfer.3\] Los conectores Transfer Family deben tener habilitado el registro](#)
- [\[Transfer.4\] Los acuerdos Transfer Family deben estar etiquetados](#)
- [\[Transfer.5\] Los certificados de Transfer Family deben estar etiquetados](#)
- [\[Transfer.6\] Los conectores Transfer Family deben estar etiquetados](#)
- [\[Transfer.7\] Los perfiles de Transfer Family deben estar etiquetados](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas de \[WAF.2\] Regionales AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.4\] Regionales AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [La AWS WAF web de \[WAF.10\] ACLs debe tener al menos una regla o grupo de reglas](#)
- [El registro de ACL AWS WAF web de \[WAF.11\] debe estar habilitado](#)
- [AWS WAF Las reglas de \[WAF.12\] deben tener habilitadas las métricas CloudWatch](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

Medio Oriente (Baréin)

Los siguientes controles no se admiten en la región de Oriente Medio (Baréin).

- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)

- [\[CloudTrail.10\] Los almacenes de datos de eventos de CloudTrail Lake deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DocumentDb.6\] Los clústeres de Amazon DocumentDB deben cifrarse en tránsito](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC220\] Ambos túneles de VPN de una conexión de AWS Site-to-Site VPN deben estar activos](#)
- [\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[ECR.5\] Los repositorios de ECR deben estar cifrados y gestionados por el cliente AWS KMS keys](#)

- [\[ECS.17\] Las definiciones de tareas de ECS no deben utilizar el modo de red host](#)
- [\[ELB.17\] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FSx.3\] FSx para los sistemas de archivos OpenZFS, debe configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[FSx.4\] FSx para los sistemas de archivos NetApp ONTAP, debe configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[FSx.5\] FSx para Windows, los sistemas de archivos del servidor de archivos deben configurarse para el despliegue en zonas de disponibilidad múltiples](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[Glue.4\] Los trabajos de AWS Glue Spark deberían ejecutarse en versiones compatibles de AWS Glue](#)
- [\[GuardDuty.11\] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada](#)
- [\[GuardDuty.12\] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada](#)
- [\[GuardDuty.13\] La monitorización del GuardDuty EC2 tiempo de ejecución debe estar habilitada](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[IoTEvents.1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoTEvents.2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoTEvents.3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoTSiteWise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoTSiteWise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)

- [\[Io TSite Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[Io TTwin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[Io TTwin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[Io TWireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de cambio de subred](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.41\] Las instancias de base de datos de RDS para SQL Server deben cifrarse en tránsito](#)
- [\[RDS.42\] Las instancias de base de datos de RDS para MariaDB deberían publicar registros en Logs CloudWatch](#)
- [\[RDS.44\] El RDS para las instancias de base de datos MariaDB debe cifrarse en tránsito](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[RedshiftServerless.3\] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público](#)
- [\[RedshiftServerless.4\] Los espacios de nombres de Redshift Serverless deben estar cifrados y gestionados por el cliente AWS KMS keys](#)
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de usuario de administrador predeterminado](#)

- [\[RedshiftServerless.6\]](#) Los espacios de nombres de Redshift Serverless deberían exportar los registros a los registros CloudWatch
- [Los espacios RedshiftServerless de nombres de Redshift Serverless no deben usar el nombre de base de datos predeterminado](#)
- [\[Route53.1\]](#) Las comprobaciones de estado de Route 53 deben estar etiquetadas
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\]](#) Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público
- [\[SageMaker.8\]](#) las instancias de SageMaker notebook deberían ejecutarse en plataformas compatibles
- [\[SQS.3\]](#) Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [\[Transfer.3\]](#) Los conectores Transfer Family deben tener habilitado el registro
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WorkSpaces.1\]](#) los volúmenes de WorkSpaces usuarios deben cifrarse en reposo
- [\[WorkSpaces.2\]](#) los volúmenes WorkSpaces raíz deben cifrarse en reposo

Medio Oriente (EAU)

Los siguientes controles no se admiten en la región de Oriente Medio (Emiratos Árabes Unidos).

- [\[APIGateway.8\]](#) Las rutas de API Gateway deben especificar un tipo de autorización
- [\[APIGateway.9\]](#) El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [\[Amplify.1\]](#) Las aplicaciones de Amplify deben estar etiquetadas
- [\[Amplify.2\]](#) Las ramas de Amplify deben estar etiquetadas
- [\[AppConfig.1\]](#) AWS AppConfig las aplicaciones deben estar etiquetadas
- [\[AppConfig.2\]](#) los perfiles de AWS AppConfig configuración deben estar etiquetados
- [\[AppConfig.3\]](#) AWS AppConfig los entornos deben estar etiquetados
- [\[AppFlow.1\]](#) AppFlow Los flujos de Amazon deben estar etiquetados

- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[AutoScaling.1\] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar las comprobaciones de estado del ELB](#)
- [\[Backup.1\] Los puntos AWS Backup de recuperación deben cifrarse en reposo](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CloudTrail.1\] CloudTrail debe habilitarse y configurarse con al menos un registro de seguimiento para varias regiones que incluya eventos de administración de lectura y escritura](#)
- [\[CloudTrail.6\] Asegurar que los CloudTrail registros del bucket de S3 no son de acceso público](#)
- [\[CloudWatch.16\] Los grupos de CloudWatch registros deben retenerse durante un periodo específico](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)

- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Cognito.1\] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.2\] Los certificados DMS deben estar etiquetados](#)
- [\[DMS.3\] Las suscripciones a eventos de DMS deben estar etiquetadas](#)
- [\[DMS.4\] Las instancias de replicación de DMS deben etiquetarse](#)
- [\[DMS.5\] Los grupos de subredes de replicación del DMS deben estar etiquetados](#)
- [\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)
- [\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)
- [\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM](#)
- [\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado](#)
- [\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC24\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.8\] EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancias IMDSv2](#)
- [\[EC2.12\] Amazon no utilizado EC2 EIPs debería retirarse](#)

- [\[EC2.14\] Los grupos de seguridad no deben permitir la entrada desde 0.0.0.0.0.0/0 o: :/0 al puerto 3389](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)
- [\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.25\] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red](#)
- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad](#)
- [\[EC251\] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.170\] Las plantillas de EC2 lanzamiento deben usar el servicio de metadatos de instancias versión 2 \(\) IMDSv2](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.175\] Las plantillas de EC2 lanzamiento deben estar etiquetadas](#)
- [\[EC2.177\] las sesiones espejo EC2 de tráfico deberían estar etiquetadas](#)
- [\[EC2.179\] Los objetivos EC2 de tráfico reflejados deben estar etiquetados](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[ECS.1\] Las definiciones de tareas de Amazon ECS deben tener modos de red seguros y definiciones de usuario](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] Los volúmenes de Amazon EFS deben estar en los planes de respaldo](#)
- [\[ELB.3\] Los oyentes de Equilibrador de carga clásico deben configurarse con una terminación HTTPS o TLS](#)
- [\[ELB.14\] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.17\] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas](#)

- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.2\] ElastiCache Los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias](#)
- [\[ElastiCache.3\] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática](#)
- [\[ElastiCache.4\] los grupos de ElastiCache replicación deben estar cifrados en reposo](#)
- [\[ElastiCache.5\] los grupos de ElastiCache replicación deben cifrarse en tránsito](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)
- [\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)
- [\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)
- [\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)
- [\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[Glue.4\] Los trabajos de AWS Glue Spark deberían ejecutarse en versiones compatibles de AWS Glue](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[IAM.1\] Las políticas de IAM no deben permitir privilegios administrativos completos “*”](#)
- [\[IAM.2\] Los usuarios de IAM no deben tener políticas de IAM asociadas](#)
- [\[IAM.3\] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos](#)
- [\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)

- [\[IAM.5\] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola](#)
- [\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)
- [\[IAM.18\] Asegurar que se ha creado un rol de soporte para administrar incidentes con AWS Support](#)
- [\[IAM.19\] MFA se debe habilitar para todos los usuarios de IAM](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)
- [\[IAM.22\] Se deben eliminar las credenciales de usuario de IAM que no se hayan utilizado durante 45 días](#)
- [\[IAM.24\] Los roles de IAM deben etiquetarse](#)
- [\[IAM.25\] Los usuarios de IAM deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IAM.27\] Las identidades de IAM no deben tener adjunta la política AWSCloud ShellFullAccess](#)
- [\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.2\] El análisis de ECR en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[Inspector.4\] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[IoTEvents .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoTEvents .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoTEvents .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoTSiteWise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoTSiteWise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[IoT TwinMaker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoT TwinMaker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoT TwinMaker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)

- [\[Io TTwin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[Io TWireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[Io TWireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)
- [\[KMS.1\] Las políticas gestionadas por los clientes de IAM no deberían permitir acciones de descifrado en todas las claves de KMS](#)
- [\[KMS.2\] Los directores de IAM no deberían tener políticas integradas de IAM que permitan realizar acciones de descifrado en todas las claves de KMS](#)
- [La rotación de AWS KMS teclas \[KMS.4\] debe estar habilitada](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)
- [Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)
- [Los OpenSearch dominios \[Opensearch.3\] deben cifrar los datos enviados entre nodos](#)
- [El registro de errores de OpenSearch dominio \[Opensearch.4\] en CloudWatch Logs debe estar activado](#)
- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)
- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los OpenSearch dominios \[Opensearch.7\] deben tener habilitado un control de acceso detallado](#)
- [\[Opensearch.8\] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente](#)
- [Los OpenSearch dominios \[Opensearch.9\] deben estar etiquetados](#)
- [Los OpenSearch dominios \[Opensearch.10\] deben tener instalada la última actualización de software](#)
- [Los OpenSearch dominios \[Opensearch.11\] deben tener al menos tres nodos principales dedicados](#)

- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [Las instancias de base de datos de RDS \[RDS.26\] deben protegerse mediante un plan de copias de seguridad](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] las instancias de SageMaker notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook](#)
- [\[SageMaker.5\] SageMaker los modelos deberían bloquear el tráfico entrante](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SQS.3\] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público](#)
- [\[SSM.1\] EC2 Las instancias de Amazon deben administrarse mediante AWS Systems Manager](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)

- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [La AWS WAF web de \[WAF.10\] ACLs debe tener al menos una regla o grupo de reglas](#)
- [El registro de ACL AWS WAF web de \[WAF.11\] debe estar habilitado](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

América del Sur (São Paulo)

Los siguientes controles no se admiten en la región de Sudamérica (São Paulo).

- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront.5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)

- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [Los perfiles de AWS IoT Device Defender seguridad \[IoT.1\] deben estar etiquetados](#)
- [\[IoT.2\] las acciones de AWS IoT Core mitigación deben estar etiquetadas](#)
- [AWS IoT Core Las dimensiones de \[IoT.3\] deben estar etiquetadas](#)
- [\[IoTEvents .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoTEvents .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoTEvents .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoTSiteWise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoTSiteWise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Twin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)

- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

AWS GovCloud (Este de EE. UU.)

Los siguientes controles no se admiten en la región AWS GovCloud (EE. UU. Este).

- [\[ACM.2\] Los certificados RSA administrados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)
- [\[Cuenta.1\] La información de contacto de seguridad debe proporcionarse para un Cuenta de AWS](#)
- [\[Account.2\] Cuentas de AWS debe formar parte de una organización AWS Organizations](#)
- [\[APIGateway.2\] Las etapas de la API de REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend](#)
- [\[APIGateway.8\] Las rutas de API Gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas V2 de API Gateway](#)
- [\[Amplify.1\] Las aplicaciones de Amplify deben estar etiquetadas](#)
- [\[Amplify.2\] Las ramas de Amplify deben estar etiquetadas](#)
- [\[AppConfig.1\] AWS AppConfig las aplicaciones deben estar etiquetadas](#)

- [\[AppConfig.2\] los perfiles de AWS AppConfig configuración deben estar etiquetados](#)
- [\[AppConfig.3\] AWS AppConfig los entornos deben estar etiquetados](#)
- [\[AppConfig.4\] Las asociaciones AWS AppConfig de extensiones deben estar etiquetadas](#)
- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.2\] AWS AppSync debe tener habilitado el registro a nivel de campo](#)
- [\[AppSync.4\] AWS AppSync APIs GraphQL debe estar etiquetado](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves de API](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[AutoScaling.2\] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad](#)
- [\[AutoScaling.3\] Las configuraciones de lanzamiento de grupos de Auto Scaling deberían configurar las EC2 instancias para que requieran la versión 2 del Servicio de Metadatos de Instancia \(IMDSv2\)](#)
- [\[AutoScaling.6\] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad](#)
- [\[AutoScaling.9\] Los grupos de Amazon EC2 Auto Scaling deberían usar las plantillas de EC2 lanzamiento de Amazon](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[Batch.1\] Las colas de trabajos por lotes deben estar etiquetadas](#)
- [\[Batch.2\] Las políticas de programación de lotes deben estar etiquetadas](#)
- [\[Batch.3\] Los entornos de procesamiento por lotes deben etiquetarse](#)
- [\[Batch.4\] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront5\] CloudFront las distribuciones deben tener el registro habilitado](#)

- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CloudWatch.17\] las acciones CloudWatch de alarma deben estar activadas](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeBuild.3\] Los registros de CodeBuild S3 deben estar cifrados](#)
- [\[CodeBuild.4\] Los entornos de los CodeBuild proyectos deben tener una duración de registro AWS Config](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Cognito.1\] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[Connect.2\] Las instancias de Amazon Connect deben tener el CloudWatch registro activado](#)
- [\[DataSync.2\] DataSync las tareas deben estar etiquetadas](#)
- [\[DMS.2\] Los certificados DMS deben estar etiquetados](#)
- [\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)
- [\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)

- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.21\] La red no ACLs debe permitir la entrada desde 0.0.0/0 al puerto 22 o al puerto 3389](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC2.24\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.25\] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red](#)
- [\[EC2.47\] Los servicios de puntos de conexión de Amazon VPC deben etiquetarse](#)
- [\[EC2.52\] Las EC2 puertas de enlace de](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.170\] Las plantillas de EC2 lanzamiento deben usar el servicio de metadatos de instancias versión 2 \(\) IMDSv2](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.174\] Los conjuntos de opciones de EC2 DHCP deben estar etiquetados](#)
- [\[EC2.175\] Las plantillas de EC2 lanzamiento deben estar etiquetadas](#)
- [\[EC2.176\] Las listas de EC2 prefijos deben estar etiquetadas](#)
- [\[EC2.177\] las sesiones espejo EC2 de tráfico deberían estar etiquetadas](#)

- [\[EC2.178\] Los filtros espejo de EC2 tráfico deben estar etiquetados](#)
- [\[EC2.179\] Los objetivos EC2 de tráfico reflejados deben estar etiquetados](#)
- [\[ECR.1\] Los repositorios privados del ECR deben tener configurado el escaneo de imágenes](#)
- [\[ECR.2\] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas](#)
- [\[ECR.3\] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[ECS.3\] Las definiciones de tareas de ECS no deben compartir el espacio de nombres de los procesos del anfitrión](#)
- [\[ECS.4\] Los contenedores de ECS deben ejecutarse sin privilegios](#)
- [\[ECS.5\] Los contenedores ECS deben limitarse al acceso de solo lectura a los sistemas de archivos raíz](#)
- [\[ECS.8\] Los secretos no deben pasarse como variables de entorno del contenedor](#)
- [\[ECS.9\] Las definiciones de tareas de ECS deben tener una configuración de registro](#)
- [\[ECS.10\] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate](#)
- [\[ECS.12\] Los clústeres de ECS deben usar Container Insights](#)
- [\[EFS.3\] Los puntos de acceso EFS deben aplicar un directorio raíz](#)
- [\[EFS.4\] Los puntos de acceso EFS deben imponer una identidad de usuario](#)
- [\[EKS.2\] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible](#)
- [\[EKS.8\] Los clústeres de EKS deben tener habilitado el registro de auditoría](#)
- [\[ELB.10\] Equilibrador de carga clásico debe abarcar varias zonas de disponibilidad](#)
- [\[ELB.12\] Equilibrador de carga de aplicación debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.13\] Los equilibradores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad](#)
- [\[ELB.14\] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.16\] Los equilibradores de carga de aplicaciones deben estar asociados a una ACL web de AWS WAF](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)

- [\[ElastiCache.2\] ElastiCache Los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias](#)
- [\[ElastiCache.3\] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática](#)
- [\[ElastiCache.4\] los grupos de ElastiCache replicación deben estar cifrados en reposo](#)
- [\[ElastiCache.5\] los grupos de ElastiCache replicación deben cifrarse en tránsito](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)
- [\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)
- [\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)
- [\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)
- [\[EMR.2\] La configuración de bloqueo del acceso público de Amazon EMR debe estar habilitada](#)
- [\[EMR.3\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo](#)
- [\[EMR.4\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito](#)
- [\[ES.4\] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros](#)
- [\[EventBridge.3\] Los autobuses de eventos EventBridge personalizados deben incluir una política basada en los recursos](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FSx.1\] en el caso FSx de OpenZFS, los sistemas de archivos deben configurarse para copiar etiquetas en copias de seguridad y volúmenes](#)
- [\[FSx.2\] FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)

- [\[Glue.3\] Las transformaciones AWS Glue de aprendizaje automático deben cifrarse en reposo](#)
- [\[GuardDuty.7\] La supervisión en tiempo de ejecución de GuardDuty EKS debe estar habilitada](#)
- [\[GuardDuty.8\] La protección contra GuardDuty malware para EC2 debe estar habilitada](#)
- [\[GuardDuty.9\] La protección de GuardDuty RDS debe estar habilitada](#)
- [\[GuardDuty.11\] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada](#)
- [\[GuardDuty.12\] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada](#)
- [\[GuardDuty.13\] La monitorización del GuardDuty EC2 tiempo de ejecución debe estar habilitada](#)
- [\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)
- [\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)
- [\[IAM.24\] Los roles de IAM deben etiquetarse](#)
- [\[IAM.25\] Los usuarios de IAM deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[IAM.28\] El analizador de acceso externo del Analizador de acceso de IAM debe habilitarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[IoTEvents .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoTEvents .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoTEvents .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoTSiteWise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoTSiteWise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoTSiteWise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[IoTThingMaker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoTThingMaker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoTThingMaker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoTThingMaker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoTWireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)

- [\[IoT Wireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)
- [\[Kinesis.1\] Las transmisiones de Kinesis deben cifrarse en reposo](#)
- [\[KMS.5\] Las claves KMS no deben ser de acceso público](#)
- [\[Lambda.5\] Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)
- [\[MQ.3\] Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[MQ.5\] Los corredores ActiveMQ deben usar el modo de implementación activo/en espera](#)
- [\[MQ.6\] Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres](#)
- [\[MSK.1\] Los clústeres de MSK deben cifrarse en tránsito entre los nodos intermediarios](#)
- [\[MSK.2\] Los clústeres de MSK deberían tener configurada una supervisión mejorada](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [\[Neptune.4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación](#)
- [\[Neptune.5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas](#)
- [\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM](#)
- [\[Neptune.8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas](#)

- [\[Neptune.9\] Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad](#)
- [Los NetworkFirewall firewalls de Network Firewall se deben implementar en varias zonas de disponibilidad](#)
- [\[NetworkFirewall.2\] El registro de Network Firewall debe estar habilitado](#)
- [\[NetworkFirewall.3\] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas](#)
- [\[NetworkFirewall.4\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos](#)
- [\[NetworkFirewall.5\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados](#)
- [El grupo de reglas de Stateless Network Firewall \[NetworkFirewall.6\] no debe estar vacío](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de eliminación](#)
- [Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)
- [Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)
- [Los OpenSearch dominios \[Opensearch.3\] deben cifrar los datos enviados entre nodos](#)
- [El registro de errores de OpenSearch dominio \[Opensearch.4\] en CloudWatch Logs debe estar activado](#)
- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)
- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los OpenSearch dominios \[Opensearch.7\] deben tener habilitado un control de acceso detallado](#)
- [\[Opensearch.8\] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente](#)
- [La autoridad emisora de certificados AWS Private CA raíz \[PCA.1\] debe estar deshabilitada](#)
- [\[PCA.2\] Se debe etiquetar a las autoridades certificadoras de CA AWS privadas](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [Los clústeres de bases de datos de RDS \[RDS.15\] deben configurarse para varias zonas de disponibilidad](#)
- [Los clústeres de bases de datos de RDS \[RDS.24\] deben usar un nombre de usuario de administrador personalizado](#)

- [Las instancias de bases de datos de RDS \[RDS.25\] deben usar un nombre de usuario de administrador personalizado](#)
- [Los clústeres de bases de datos de RDS \[RDS.27\] deben cifrarse en reposo](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[RDS.34\] Los clústeres de bases de datos Aurora MySQL deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)
- [Los clústeres de Amazon Redshift \[Redshift.8\] no deben usar el nombre de usuario de administrador predeterminado](#)
- [Los clústeres de Redshift \[Redshift.9\] no deben usar el nombre de base de datos predeterminado](#)
- [Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo](#)
- [\[Redshift.17\] Los grupos de parámetros del clúster de Redshift deben estar etiquetados](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)
- [\[RedshiftServerless.2\] Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL](#)
- [\[RedshiftServerless.3\] Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público](#)
- [\[RedshiftServerless.6\] Los espacios de nombres de Redshift Serverless deberían exportar los registros a los registros CloudWatch](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [Las zonas alojadas públicas de Route 53 \[Route53.2\] deben registrar las consultas de DNS](#)
- [\[S3.10\] Los buckets de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida](#)
- [\[S3.11\] Los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos](#)
- [\[S3.12\] no ACLs debe usarse para administrar el acceso de los usuarios a los depósitos de uso general de S3](#)
- [\[S3.13\] Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida](#)
- [\[S3.20\] Los buckets de uso general de S3 deben tener habilitada la eliminación de MFA](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)

- [\[SageMaker.1\] Las instancias de Amazon SageMaker Notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] las instancias de SageMaker notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook](#)
- [\[SageMaker.5\] SageMaker los modelos deberían bloquear el tráfico entrante](#)
- [\[SageMaker.6\] Las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas](#)
- [\[SageMaker.7\] SageMaker las imágenes deben estar etiquetadas](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [\[SNS.4\] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público](#)
- [\[SQS.3\] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público](#)
- [\[SSM.4\] Los documentos SSM no deben ser públicos](#)
- [\[SSM.5\] Los documentos SSM deben estar etiquetados](#)
- [\[StepFunctions.1\] Las máquinas de estado de Step Functions deberían tener el registro activado](#)
- [\[StepFunctions.2\] Las actividades de Step Functions deben estar etiquetadas](#)
- [\[Transfer.4\] Los acuerdos Transfer Family deben estar etiquetados](#)
- [\[Transfer.5\] Los certificados de Transfer Family deben estar etiquetados](#)
- [\[Transfer.6\] Los conectores Transfer Family deben estar etiquetados](#)
- [\[Transfer.7\] Los perfiles de Transfer Family deben estar etiquetados](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas de \[WAF.2\] Regionales AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.4\] Regionales AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [La AWS WAF web de \[WAF.10\] ACLs debe tener al menos una regla o grupo de reglas](#)

- [\[AWS WAF Las reglas de \[WAF.12\] deben tener habilitadas las métricas CloudWatch](#)
- [\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo](#)
- [\[WorkSpaces.2\] los volúmenes WorkSpaces raíz deben cifrarse en reposo](#)

AWS GovCloud (EEUU-Oeste)

Los siguientes controles no se admiten en la región AWS GovCloud (EE. UU. Oeste).

- [\[ACM.2\] Los certificados RSA administrados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)
- [\[Cuenta.1\] La información de contacto de seguridad debe proporcionarse para un Cuenta de AWS](#)
- [\[Account.2\] Cuentas de AWS debe formar parte de una organización AWS Organizations](#)
- [\[APIGateway.2\] Las etapas de la API de REST de API Gateway deben configurarse para usar certificados SSL para la autenticación de backend](#)
- [\[APIGateway.8\] Las rutas de API Gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas V2 de API Gateway](#)
- [\[Amplify.1\] Las aplicaciones de Amplify deben estar etiquetadas](#)
- [\[Amplify.2\] Las ramas de Amplify deben estar etiquetadas](#)
- [\[AppConfig.1\] AWS AppConfig las aplicaciones deben estar etiquetadas](#)
- [\[AppConfig.2\] los perfiles de AWS AppConfig configuración deben estar etiquetados](#)
- [\[AppConfig.3\] AWS AppConfig los entornos deben estar etiquetados](#)
- [\[AppConfig.4\] Las asociaciones AWS AppConfig de extensiones deben estar etiquetadas](#)
- [\[AppFlow.1\] AppFlow Los flujos de Amazon deben estar etiquetados](#)
- [\[AppRunner.1\] Los servicios de App Runner deben estar etiquetados](#)
- [\[AppRunner.2\] Los conectores VPC de App Runner deben estar etiquetados](#)
- [\[AppSync.1\] Las cachés de las AWS AppSync API deben cifrarse en reposo](#)
- [\[AppSync.2\] AWS AppSync debe tener habilitado el registro a nivel de campo](#)
- [\[AppSync.4\] AWS AppSync APIs GraphQL debe estar etiquetado](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves de API](#)
- [\[AppSync.6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito](#)
- [\[AutoScaling.2\] El grupo Amazon EC2 Auto Scaling debe cubrir varias zonas de disponibilidad](#)

- [\[AutoScaling.3\] Las configuraciones de lanzamiento de grupos de Auto Scaling deberían configurar las EC2 instancias para que requieran la versión 2 del Servicio de Metadatos de Instancia \(IMDSv2\)](#)
- [\[AutoScaling.6\] Los grupos de Auto Scaling deben usar varios tipos de instancias en múltiples zonas de disponibilidad](#)
- [\[AutoScaling.9\] Los grupos de Amazon EC2 Auto Scaling deberían usar las plantillas de EC2 lanzamiento de Amazon](#)
- [\[Backup.4\] los planes de AWS Backup informes deben estar etiquetados](#)
- [\[Batch.1\] Las colas de trabajos por lotes deben estar etiquetadas](#)
- [\[Batch.2\] Las políticas de programación de lotes deben estar etiquetadas](#)
- [\[Batch.3\] Los entornos de procesamiento por lotes deben etiquetarse](#)
- [\[Batch.4\] Las propiedades de los recursos de cómputo en los entornos de cómputo por lotes gestionados deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deben requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront Las distribuciones deben tener configurada la conmutación por error de origen](#)
- [\[CloudFront5\] CloudFront las distribuciones deben tener el registro habilitado](#)
- [\[CloudFront.6\] CloudFront Las distribuciones deben tener WAF habilitado](#)
- [\[CloudFront.7\] CloudFront Las distribuciones deben usar certificados SSL/TLS personalizados](#)
- [\[CloudFront.8\] CloudFront Las distribuciones deben usar SNI para atender solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront Las distribuciones deben cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront Las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones periféricas y los orígenes personalizados](#)
- [\[CloudFront.12\] CloudFront Las distribuciones no deben apuntar a orígenes S3 inexistentes](#)
- [\[CloudFront.13\] CloudFront Las distribuciones deben usar el control de acceso de origen](#)
- [\[CloudFront.14\] CloudFront Las distribuciones deben etiquetarse](#)
- [\[CloudWatch.17\] las acciones CloudWatch de alarma deben estar activadas](#)
- [\[CodeArtifact.1\] CodeArtifact Los repositorios deben estar etiquetados](#)
- [\[CodeBuild.3\] Los registros de CodeBuild S3 deben estar cifrados](#)

- [\[CodeBuild.4\] Los entornos de los CodeBuild proyectos deben tener una duración de registro AWS Config](#)
- [\[CodeGuruProfiler.1\] Los grupos de CodeGuru creación de perfiles de Profiler deben estar etiquetados](#)
- [\[CodeGuruReviewer.1\] Las asociaciones de repositorios de CodeGuru Reviewer deben estar etiquetadas](#)
- [\[Cognito.1\] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar](#)
- [\[Connect.1\] Los tipos de objetos de los perfiles de clientes de Amazon Connect deben estar etiquetados](#)
- [\[DataSync.2\] DataSync las tareas deben estar etiquetadas](#)
- [\[DMS.2\] Los certificados DMS deben estar etiquetados](#)
- [\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro](#)
- [\[DMS.9\] Los puntos finales del DMS deben usar SSL](#)
- [\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo](#)
- [\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DocumentDb.4\] Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch](#)
- [\[DocumentDb.5\] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(DAX\) deben cifrarse en reposo](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.21\] La red no ACLs debe permitir la entrada desde 0.0.0/0 al puerto 22 o al puerto 3389](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon que no se utilicen deben eliminarse](#)

- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC224\] No se deben utilizar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.25\] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red](#)
- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad](#)
- [\[EC2.38\] EC2 las instancias deben estar etiquetadas](#)
- [\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager](#)
- [\[EC2.60\] VPCs debe configurarse con un punto final de interfaz para Systems Manager Incident Manager](#)
- [\[EC2.170\] Las plantillas de EC2 lanzamiento deben usar el servicio de metadatos de instancias versión 2 \(\) IMDSv2](#)
- [\[EC2.173\] Las solicitudes de EC2 Spot Fleet deberían permitir el cifrado de los volúmenes de EBS adjuntos](#)
- [\[EC2.174\] Los conjuntos de opciones de EC2 DHCP deben estar etiquetados](#)
- [\[EC2.175\] Las plantillas de EC2 lanzamiento deben estar etiquetadas](#)
- [\[EC2.176\] Las listas de EC2 prefijos deben estar etiquetadas](#)
- [\[EC2.177\] las sesiones espejo EC2 de tráfico deberían estar etiquetadas](#)
- [\[EC2.178\] Los filtros espejo de EC2 tráfico deben estar etiquetados](#)
- [\[EC2.179\] Los objetivos EC2 de tráfico reflejados deben estar etiquetados](#)
- [\[ECR.1\] Los repositorios privados del ECR deben tener configurado el escaneo de imágenes](#)
- [\[ECR.2\] Los repositorios privados de ECR deben tener configurada la inmutabilidad de etiquetas](#)
- [\[ECR.3\] Los repositorios de ECR deben tener configurada al menos una política de ciclo de vida](#)
- [\[ECR.4\] Los repositorios públicos de ECR deben estar etiquetados](#)
- [\[ECS.3\] Las definiciones de tareas de ECS no deben compartir el espacio de nombres de los procesos del anfitrión](#)
- [\[ECS.4\] Los contenedores de ECS deben ejecutarse sin privilegios](#)
- [\[ECS.5\] Los contenedores ECS deben limitarse al acceso de solo lectura a los sistemas de archivos raíz](#)
- [\[ECS.8\] Los secretos no deben pasarse como variables de entorno del contenedor](#)
- [\[ECS.9\] Las definiciones de tareas de ECS deben tener una configuración de registro](#)

- [\[ECS.10\] Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate](#)
- [\[ECS.12\] Los clústeres de ECS deben usar Container Insights](#)
- [\[EFS.3\] Los puntos de acceso EFS deben aplicar un directorio raíz](#)
- [\[EFS.4\] Los puntos de acceso EFS deben imponer una identidad de usuario](#)
- [\[EKS.2\] Los clústeres de EKS deberían ejecutarse en una versión de Kubernetes compatible](#)
- [\[EKS.8\] Los clústeres de EKS deben tener habilitado el registro de auditoría](#)
- [\[ELB.10\] Equilibrador de carga clásico debe abarcar varias zonas de disponibilidad](#)
- [\[ELB.12\] Equilibrador de carga de aplicación debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.13\] Los equilibradores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad](#)
- [\[ELB.14\] El Equilibrador de carga clásico debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.16\] Los equilibradores de carga de aplicaciones deben estar asociados a una ACL web de AWS WAF](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(Redis OSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.2\] ElastiCache Los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias](#)
- [\[ElastiCache.3\] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática](#)
- [\[ElastiCache.4\] los grupos de ElastiCache replicación deben estar cifrados en reposo](#)
- [\[ElastiCache.5\] los grupos de ElastiCache replicación deben cifrarse en tránsito](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS](#)
- [\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)
- [\[ElasticBeanstalk.1\] Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados](#)
- [\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)

- [\[EMR.2\] La configuración de bloqueo del acceso público de Amazon EMR debe estar habilitada](#)
- [\[EMR.3\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo](#)
- [\[EMR.4\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito](#)
- [\[ES.4\] Debe estar habilitado el registro de errores de dominio de Elasticsearch en los CloudWatch registros](#)
- [\[EventBridge.3\] Los autobuses de eventos EventBridge personalizados deben incluir una política basada en los recursos](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FraudDetector.1\] Los tipos de entidades de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.2\] Las etiquetas de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FraudDetector.3\] Los resultados de Amazon Fraud Detector deben estar etiquetados](#)
- [\[FraudDetector.4\] Las variables de Amazon Fraud Detector deben estar etiquetadas](#)
- [\[FSx.1\] en el caso FSx de OpenZFS, los sistemas de archivos deben configurarse para copiar etiquetas en copias de seguridad y volúmenes](#)
- [\[FSx.2\] FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben estar etiquetados](#)
- [\[GuardDuty.7\] La supervisión en tiempo de ejecución de GuardDuty EKS debe estar habilitada](#)
- [\[GuardDuty.8\] La protección contra GuardDuty malware para EC2 debe estar habilitada](#)
- [\[GuardDuty.9\] La protección de GuardDuty RDS debe estar habilitada](#)
- [\[GuardDuty.11\] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada](#)
- [\[GuardDuty.12\] La monitorización del tiempo de ejecución de GuardDuty ECS debe estar habilitada](#)
- [\[GuardDuty.13\] La monitorización del GuardDuty EC2 tiempo de ejecución debe estar habilitada](#)
- [\[PCI.IAM.6\] La MFA de hardware debe estar habilitada para el usuario raíz](#)
- [\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)
- [\[IAM.24\] Los roles de IAM deben etiquetarse](#)
- [\[IAM.25\] Los usuarios de IAM deben etiquetarse](#)
- [\[IAM.28\] El analizador de acceso externo del Analizador de acceso de IAM debe habilitarse](#)

- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[IoT Events .1\] Las entradas de AWS IoT Events deben estar etiquetadas](#)
- [\[IoT Events .2\] Los modelos de detectores de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Events .3\] Los modelos de alarma de AWS IoT Events deben estar etiquetados](#)
- [\[IoT Site Wise.1\] Los modelos de SiteWise activos de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.2\] SiteWise Los paneles de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.3\] SiteWise Las pasarelas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Site Wise.4\] Los SiteWise portales de AWS IoT deben estar etiquetados](#)
- [\[IoT Site Wise.5\] Los SiteWise proyectos de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoT Twin Maker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoT Twin Maker.4\] TwinMaker Las entidades de AWS IoT deben estar etiquetadas](#)
- [\[IoT Wireless .1\] Los grupos de multidifusión de AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .2\] Los perfiles del servicio AWS IoT Wireless deben estar etiquetados](#)
- [\[IoT Wireless .3\] Las tareas de AWS IoT FUOTA deben estar etiquetadas](#)
- [\[IVS.1\] Los pares de teclas de reproducción del IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales de IVS deben estar etiquetados](#)
- [\[Keyspaces.1\] Los espacios clave de Amazon Keyspaces deben estar etiquetados](#)
- [\[Kinesis.1\] Las transmisiones de Kinesis deben cifrarse en reposo](#)
- [\[KMS.5\] Las claves KMS no deben ser de acceso público](#)
- [\[Lambda.5\] Las funciones de Lambda de la VPC deben funcionar en varias zonas de disponibilidad](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)
- [\[MQ.3\] Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[MQ.5\] Los corredores ActiveMQ deben usar el modo de implementación activo/en espera](#)
- [\[MQ.6\] Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres](#)
- [\[MSK.1\] Los clústeres de MSK deben cifrarse en tránsito entre los nodos intermediarios](#)

- [\[MSK.2\] Los clústeres de MSK deberían tener configurada una supervisión mejorada](#)
- [\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito](#)
- [\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [\[Neptune.4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación](#)
- [\[Neptune.5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas](#)
- [\[Neptune.6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo](#)
- [\[Neptune.7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM](#)
- [\[Neptune.8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas](#)
- [\[Neptune.9\] Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad](#)
- [Los NetworkFirewall firewalls de Network Firewall se deben implementar en varias zonas de disponibilidad](#)
- [\[NetworkFirewall.2\] El registro de Network Firewall debe estar habilitado](#)
- [\[NetworkFirewall.3\] Las políticas de Network Firewall deben tener asociado al menos un grupo de reglas](#)
- [\[NetworkFirewall.4\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes completos](#)
- [\[NetworkFirewall.5\] La acción sin estado predeterminada para las políticas de Network Firewall debe ser eliminar o reenviar paquetes fragmentados](#)
- [El grupo de reglas de Stateless Network Firewall \[NetworkFirewall.6\] no debe estar vacío](#)
- [Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de eliminación](#)
- [Los OpenSearch dominios \[Opensearch.1\] deben tener activado el cifrado en reposo](#)
- [Los OpenSearch dominios \[Opensearch.2\] no deben ser de acceso público](#)
- [Los OpenSearch dominios \[Opensearch.3\] deben cifrar los datos enviados entre nodos](#)

- [El registro de errores de OpenSearch dominio \[Opensearch.4\] en CloudWatch Logs debe estar activado](#)
- [Los OpenSearch dominios \[Opensearch.5\] deben tener habilitado el registro de auditoría](#)
- [Los OpenSearch dominios \[Opensearch.6\] deben tener al menos tres nodos de datos](#)
- [Los OpenSearch dominios \[Opensearch.7\] deben tener habilitado un control de acceso detallado](#)
- [\[Opensearch.8\] Las conexiones a los OpenSearch dominios deben cifrarse según la política de seguridad TLS más reciente](#)
- [La autoridad emisora de certificados AWS Private CA raíz \[PCA.1\] debe estar deshabilitada](#)
- [\[PCA.2\] Se debe etiquetar a las autoridades certificadoras de CA AWS privadas](#)
- [Los clústeres de Amazon Aurora \[RDS.14\] deben tener habilitada la característica de búsqueda de datos anteriores](#)
- [Los clústeres de bases de datos de RDS \[RDS.15\] deben configurarse para varias zonas de disponibilidad](#)
- [Los clústeres de bases de datos de RDS \[RDS.24\] deben usar un nombre de usuario de administrador personalizado](#)
- [Las instancias de bases de datos de RDS \[RDS.25\] deben usar un nombre de usuario de administrador personalizado](#)
- [Los clústeres de bases de datos de RDS \[RDS.27\] deben cifrarse en reposo](#)
- [\[RDS.34\] Los clústeres de bases de datos Aurora MySQL deberían publicar los registros de auditoría en Logs CloudWatch](#)
- [Los clústeres de bases de datos de RDS \[RDS.35\] deben tener habilitada la actualización automática de las versiones secundarias](#)
- [Los clústeres de Redshift \[Redshift.7\] deberían utilizar un enrutamiento de VPC mejorado](#)
- [Los clústeres de Amazon Redshift \[Redshift.8\] no deben usar el nombre de usuario de administrador predeterminado](#)
- [Los clústeres de Redshift \[Redshift.9\] no deben usar el nombre de base de datos predeterminado](#)
- [Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo](#)
- [\[Redshift.11\] Los clústeres de Redshift deben etiquetarse](#)
- [\[Redshift.13\] Las instantáneas del clúster de Redshift deben etiquetarse](#)
- [\[Redshift.17\] Los grupos de parámetros del clúster de Redshift deben estar etiquetados](#)
- [Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado](#)

- [\[RedshiftServerless.2\]](#) Las conexiones a los grupos de trabajo sin servidor de Redshift deberían ser obligatorias para usar SSL
- [\[RedshiftServerless.3\]](#) Los grupos de trabajo sin servidor de Redshift deberían prohibir el acceso público
- [\[RedshiftServerless.6\]](#) Los espacios de nombres de Redshift Serverless deberían exportar los registros a los registros CloudWatch
- [\[Route53.1\]](#) Las comprobaciones de estado de Route 53 deben estar etiquetadas
- [Las zonas alojadas públicas de Route 53 \[Route53.2\]](#) deben registrar las consultas de DNS
- [\[S3.10\]](#) Los buckets de uso general de S3 con el control de versiones habilitado deben tener configuraciones de ciclo de vida
- [\[S3.11\]](#) Los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos
- [\[S3.12\]](#) no ACLs debe usarse para administrar el acceso de los usuarios a los depósitos de uso general de S3
- [\[S3.13\]](#) Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida
- [\[S3.20\]](#) Los buckets de uso general de S3 deben tener habilitada la eliminación de MFA
- [\[S3.24\]](#) Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público
- [\[SageMaker.2\]](#) las instancias de SageMaker notebook deben lanzarse en una VPC personalizada
- [\[SageMaker.3\]](#) Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook
- [\[SageMaker.5\]](#) SageMaker los modelos deberían bloquear el tráfico entrante
- [\[SageMaker.6\]](#) Las configuraciones de imagen de la SageMaker aplicación deben estar etiquetadas
- [\[SageMaker.7\]](#) SageMaker las imágenes deben estar etiquetadas
- [\[SNS.4\]](#) Las políticas de acceso a los temas de SNS no deberían permitir el acceso público
- [\[SQS.3\]](#) Las políticas de acceso a las colas de SQS no deberían permitir el acceso público
- [\[SSM.4\]](#) Los documentos SSM no deben ser públicos
- [\[SSM.5\]](#) Los documentos SSM deben estar etiquetados
- [\[StepFunctions.1\]](#) Las máquinas de estado de Step Functions deberían tener el registro activado
- [\[StepFunctions.2\]](#) Las actividades de Step Functions deben estar etiquetadas
- [\[Transfer.4\]](#) Los acuerdos Transfer Family deben estar etiquetados
- [\[Transfer.5\]](#) Los certificados de Transfer Family deben estar etiquetados

- [\[Transfer.6\] Los conectores Transfer Family deben estar etiquetados](#)
- [\[Transfer.7\] Los perfiles de Transfer Family deben estar etiquetados](#)
- [El registro AWS WAF Classic Global Web ACL de \[WAF.1\] debe estar habilitado](#)
- [Las reglas de \[WAF.2\] Regionales AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas de \[WAF.3\] Regionales AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.4\] Regionales AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [Las reglas globales de \[WAF.6\] AWS WAF clásicas deben tener al menos una condición](#)
- [Los grupos de reglas globales de \[WAF.7\] AWS WAF clásicos deben tener al menos una regla](#)
- [La web de \[WAF.8\] global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [La AWS WAF web de \[WAF.10\] ACLs debe tener al menos una regla o grupo de reglas](#)
- [AWS WAF Las reglas de \[WAF.12\] deben tener habilitadas las métricas CloudWatch](#)

Creación de recursos CSPM de Security Hub con CloudFormation

AWS Security Hub Cloud Security Posture Management (CSPM) se integra con AWS CloudFormation, un servicio que le ayuda a modelar y configurar sus AWS recursos para que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Cree una plantilla que describa todos los AWS recursos que desee (como las reglas de automatización) y AWS CloudFormation aprovisiona y configura esos recursos por usted.

Cuando la utilice AWS CloudFormation, podrá reutilizar la plantilla para configurar los recursos de CSPM de su Security Hub de forma coherente y repetida. Describa sus recursos una vez y, a continuación, aprovisiona los mismos recursos una y otra vez en varias regiones Cuentas de AWS .

Security Hub, CSPM y plantillas AWS CloudFormation

Para aprovisionar y configurar recursos para Security Hub CSPM y servicios relacionados, debe comprender cómo funcionan [AWS CloudFormation las plantillas](#). Las plantillas son archivos de texto en formato JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus AWS CloudFormation pilas.

Si no estás familiarizado con JSON o YAML, puedes usar AWS CloudFormation Designer para ayudarte a empezar con AWS CloudFormation las plantillas. Para obtener más información, consulta [¿Qué es AWS CloudFormation Designer?](#) en la Guía AWS CloudFormation del usuario.

Puede crear AWS CloudFormation plantillas para los siguientes tipos de recursos CSPM de Security Hub:

- Activación de Security Hub CSPM
- Designación del administrador delegado de Security Hub (CSPM) para una organización
- Especifique la forma en que está configurada su organización en Security Hub (CSPM).
- Habilitación de un estándar de seguridad
- Habilitación de agregación entre regiones
- Crear una política de configuración central y asociarla a las cuentas, a la unidad organizativa (OUs) o a la raíz
- Creación de hallazgos personalizados

- Creación de una regla de automatización
- Personalización de parámetros de control
- Suscripción a una integración de productos de terceros

Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para recursos, consulta la [referencia del tipo de recurso AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) en la Guía del AWS CloudFormation usuario.

Más información sobre AWS CloudFormation

Para obtener más información AWS CloudFormation, consulte los siguientes recursos:

- [AWS CloudFormation](#)
- [AWS CloudFormation Guía del usuario](#)
- [AWS CloudFormation Referencia de la API](#)
- [AWS CloudFormation Guía del usuario de la interfaz de línea de comandos](#)

Suscripción a los anuncios de CSPM de Security Hub con Amazon SNS

En esta sección se proporciona información sobre cómo suscribirse a los AWS anuncios de Security Hub Cloud Security Posture Management (CSPM) con Amazon Simple Notification Service (Amazon SNS) para recibir notificaciones sobre Security Hub CSPM.

Tras suscribirse, recibirá notificaciones sobre los siguientes eventos (tenga en cuenta el `AnnouncementType` correspondiente a cada evento):

- **GENERAL**— Notificaciones generales sobre el servicio CSPM de Security Hub.
- **UPCOMING_STANDARDS_CONTROLS**— Próximamente se publicarán los controles o estándares CSPM específicos de Security Hub. Este tipo de anuncio lo ayuda a preparar los flujos de trabajo de respuesta y corrección antes del lanzamiento.
- **NEW_REGIONS**— Support for Security Hub CSPM está disponible en una nueva versión. Región de AWS
- **NEW_STANDARDS_CONTROLS**— Se han agregado nuevos controles o estándares CSPM de Security Hub.
- **UPDATED_STANDARDS_CONTROLS**— Se han actualizado los controles o estándares CSPM de Security Hub existentes.
- **RETIRED_STANDARDS_CONTROLS**— Se han retirado los controles o estándares CSPM de Security Hub existentes.
- **UPDATED_ASFF**— Se han actualizado la sintaxis, los campos o los valores del formato de búsqueda de seguridad (ASFF).
- **NEW_INTEGRATION**— Están disponibles nuevas integraciones con otros AWS servicios o productos de terceros.
- **NEW_FEATURE**— Están disponibles las nuevas funciones CSPM de Security Hub.
- **UPDATED_FEATURE**— Se han actualizado las funciones CSPM de Security Hub existentes.

Las notificaciones están disponibles en todos los formatos que admite Amazon SNS. Puedes suscribirte a los anuncios de CSPM de Security Hub en todos los sitios en los [Regiones de AWS que Security Hub CSPM esté disponible](#).

Un usuario debe disponer de permisos de `Subscribe` para suscribirse a un tema de Amazon SNS. Puede lograrlo con las políticas de Amazon SNS, las políticas de IAM o ambas. Para obtener más información, consulte [Uso en conjunto de políticas y roles de IAM y Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

 Note

Security Hub CSPM envía anuncios de Amazon SNS sobre las actualizaciones del servicio CSPM de Security Hub a todos los suscriptores. Cuenta de AWS Para recibir notificaciones sobre los hallazgos del CSPM de Security Hub, consulte. [Revisión de los detalles y el historial de búsquedas en Security Hub \(CSPM\)](#)

Puede suscribirse a una cola de Amazon Simple Queue Service (Amazon SQS) sobre un tema de Amazon SNS, pero debe utilizar un tema de Amazon SNS nombre de recurso de Amazon (ARN) que se encuentre en la misma región. Para obtener más información, consulte el [tema Suscribirse una cola a un Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Queue Service.

También puede utilizar una AWS Lambda función para invocar eventos cuando reciba notificaciones. Para obtener más información, incluido un ejemplo de código de función, consulte el [Tutorial: Uso AWS Lambda con Amazon Simple Notification Service](#) en la Guía para AWS Lambda desarrolladores.

El tema de Amazon SNS ARNs para cada región es el siguiente.

Región de AWS	ARN del tema de Amazon SNS
Este de EE. UU. (Ohio)	<code>arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements</code>
Este de EE. UU. (Norte de Virginia)	<code>arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements</code>
Oeste de EE. UU. (Norte de California)	<code>arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements</code>

Región de AWS	ARN del tema de Amazon SNS
Oeste de EE. UU. (Oregón)	<code>arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements</code>
África (Ciudad del Cabo)	<code>arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements</code>
Asia-Pacífico (Hong Kong)	<code>arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements</code>
Asia-Pacífico (Hyderabad)	<code>arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements</code>
Asia-Pacífico (Yakarta)	<code>arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements</code>
Asia-Pacífico (Bombay)	<code>arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements</code>
Asia-Pacífico (Osaka)	<code>arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements</code>
Asia-Pacífico (Seúl)	<code>arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements</code>
Asia-Pacífico (Singapur)	<code>arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements</code>

Región de AWS	ARN del tema de Amazon SNS
Asia-Pacífico (Sídney)	<code>arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements</code>
Asia-Pacífico (Tokio)	<code>arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements</code>
Canadá (centro)	<code>arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements</code>
China (Pekín)	<code>arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements</code>
China (Ningxia)	<code>arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements</code>
Europa (Fráncfort)	<code>arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements</code>
Europa (Irlanda)	<code>arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements</code>
Europa (Londres)	<code>arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements</code>
Europa (Milán)	<code>arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements</code>

Región de AWS	ARN del tema de Amazon SNS
Europa (París)	<code>arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements</code>
Europa (España)	<code>arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements</code>
Europa (Estocolmo)	<code>arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements</code>
Europa (Zúrich)	<code>arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements</code>
Israel (Tel Aviv)	<code>arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements</code>
Medio Oriente (Baréin)	<code>arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements</code>
Medio Oriente (EAU)	<code>arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements</code>
América del Sur (São Paulo)	<code>arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements</code>
AWS GovCloud (Este de EE. UU.)	<code>arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements</code>

Región de AWS	ARN del tema de Amazon SNS
AWS GovCloud (Estados Unidos-Oeste)	<code>arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements</code>

Los mensajes suelen ser los mismos en todas las regiones de una [partición](#), por lo que puede suscribirse a una región de cada partición para recibir anuncios que afecten a todas las regiones de esa partición. Los anuncios asociados a las cuentas miembro no se replican en la cuenta de administrador. Como resultado, cada cuenta, incluida la cuenta de administrador, tendrá una única copia de cada anuncio. Puede decidir qué cuenta quiere usar para suscribirse a los anuncios de CSPM de Security Hub.

[Para obtener información sobre el costo de suscribirse a los anuncios de CSPM de Security Hub, consulte los precios de Amazon SNS.](#)

Suscripción a los anuncios de CSPM de Security Hub (consola)

1. [Abra la consola Amazon SNS en https://console.aws.amazon.com/sns/ la versión 3/home.](https://console.aws.amazon.com/sns/la-versión-3/home)
2. En la lista de regiones, elija la región en la que desee suscribirse a los anuncios de CSPM de Security Hub. En este ejemplo se utiliza la región us-west-2.
3. En el panel de navegación, seleccione Suscripciones y, a continuación, elija Crear suscripción.
4. Escriba el ARN del tema en el cuadro de texto ARN del tema. Por ejemplo, `arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`.
5. En Protocolo, elija cómo desea recibir los anuncios de CSPM de Security Hub. Si elige Correo electrónico, en Punto de conexión, introduzca la dirección de correo electrónico que desee usar para recibir anuncios.
6. Seleccione Crear suscripción.
7. Confirme la suscripción. Por ejemplo, si ha elegido un protocolo de correo electrónico, Amazon SNS enviará un mensaje de confirmación de la suscripción a la dirección de correo electrónico facilitada.

Suscripción a los anuncios de CSPM de Security Hub (AWS CLI)

1. Ejecuta el siguiente comando:

```
aws sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-endpoint your_email@your_domain.com
```

2. Confirme la suscripción. Por ejemplo, si ha elegido un protocolo de correo electrónico, Amazon SNS enviará un mensaje de confirmación de la suscripción a la dirección de correo electrónico facilitada.

Formato de los mensajes de Amazon SNS

Los siguientes ejemplos muestran los anuncios de CSPM de Security Hub de Amazon SNS sobre la introducción de nuevos controles de seguridad. El contenido de los mensajes varía según el tipo de anuncio, pero el formato es el mismo para todos los tipos de anuncios. Opcionalmente, se puede incluir un campo de Link que proporcione detalles sobre el anuncio.

Ejemplo: anuncio de CSPM de Security Hub para nuevos controles (protocolo de correo electrónico)

```
{
  "AnnouncementType": "NEW_STANDARDS_CONTROLS",
  "Title": "[New Controls] 36 new Security Hub CSPM controls added to the AWS Foundational Security Best Practices standard",
  "Description": "We have added 36 new controls to the AWS Foundational Security Best Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), AWS CloudFormation (CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3, NetworkFirewall.4, NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift (Redshift.9), Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS Foundational Security Best Practices standard in an account and configured Security Hub CSPM to automatically enable new controls, these controls are enabled by default. Availability of controls can vary by Region. "
}
```

Ejemplo: anuncio de CSPM de Security Hub para nuevos controles (protocolo Email-JSON)

```
{
  "Type" : "Notification",
  "MessageId" : "d124c9cf-326a-5931-9263-92a92e7af49f",
  "TopicArn" : "arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements",
  "Message" : "{\"AnnouncementType\":\"NEW_STANDARDS_CONTROLS\",\"Title\":\"[New Controls] 36 new Security Hub CSPM controls added to the AWS Foundational Security Best Practices standard\",\"Description\":\"We have added 36 new controls to the AWS Foundational Security Best Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), AWS CloudFormation (CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.1.3, NetworkFirewall.1.4, NetworkFirewall.1.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift (Redshift.9), Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS Foundational Security Best Practices standard in an account and configured SSecurity Hub CSPM to automatically enable new controls, these controls are enabled by default. Availability of controls can vary by Region. \"}",
  "Timestamp" : "2022-08-04T19:11:12.652Z",
  "SignatureVersion" : "1",
  "Signature" :
    "HTHgNFRYMetCvisulgLm4CVySvK9qCXFPHQDxYl9tuCFQuIrd7Y04m4YFR28XKMgzqrF20YP
    +EilipUm2S0TpEEt0TekU5bn74+YmNZfwr4aPFx0vUuQCV0shmHl37hjkiLjhCg/t53QQiLFP7MH
    +MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUs0G8yiJVCBEJhJ1yS
    +gkwJdhRk2UQab9RcAmE6C0K3hRWcjDwqTXz5nR6Ywv1ZqZfLI17gYKslt+jsyd/k+7k0qGm0JRD7qhE7H
    +7vaGRL0ptsQnbW8VmeYnDbahE08FV+Mp1rpV+7Qg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
    SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
    Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
    west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}
```

Desactivación de Security Hub CSPM

Puede deshabilitar AWS Security Hub Cloud Security Posture Management (CSPM) mediante la consola CSPM de Security Hub o la API de Security Hub. Si deshabilita el CSPM de Security Hub, podrá volver a habilitarlo más adelante.

Si su organización utiliza la configuración central, el administrador delegado de CSPM del Security Hub puede crear políticas de configuración que inhabiliten el Security Hub CSPM para cuentas y unidades organizativas específicas (OUs) y mantener el Security Hub CSPM activado para otras. Las políticas de configuración afectan a la región de origen y a todas las regiones vinculadas. Para obtener más información, consulte [Descripción de la configuración central en Security Hub \(CSPM\)](#).

Si deshabilita el CSPM de Security Hub para una cuenta, ocurre lo siguiente:

- Todos los estándares y controles están deshabilitados para la cuenta.
- Security Hub CSPM deja de generar e ingerir nuevos hallazgos para la cuenta.
- Transcurridos 30 días, Security Hub CSPM elimina permanentemente todos los hallazgos archivados existentes de la cuenta. Los hallazgos no se pueden recuperar mediante Security Hub CSPM.
- Transcurridos 90 días, Security Hub CSPM elimina permanentemente todos los hallazgos activos existentes en la cuenta. Los hallazgos no se pueden recuperar mediante Security Hub CSPM.
- Transcurridos 90 días, Security Hub CSPM elimina permanentemente todos los conocimientos existentes y los ajustes de configuración de CSPM de Security Hub de la cuenta. Los datos y la configuración no se pueden recuperar.

Para conservar los hallazgos existentes, puede exportarlos a un bucket de S3 antes de deshabilitar Security Hub CSPM. Puedes hacerlo mediante una acción personalizada con una EventBridge regla de Amazon. Para obtener más información, consulte [Uso EventBridge para respuesta y remediación automatizadas](#).

Si vuelves a activar el CSPM de Security Hub en un plazo de 90 días a partir de su desactivación para una cuenta, recuperarás el acceso a los hallazgos activos existentes, así como a la información y a los ajustes de configuración del CSPM de Security Hub para la cuenta. Si vuelves a activar Security Hub CSPM en un plazo de 30 días, también recuperarás el acceso a las conclusiones archivadas existentes de la cuenta. Sin embargo, los resultados existentes pueden ser inexactos porque reflejarán el estado de su AWS entorno cuando deshabilitó Security Hub CSPM. Además,

al volver a habilitar los estándares y controles individuales, Security Hub CSPM podría generar inicialmente resultados duplicados para AWS recursos específicos, en función de los estándares y controles que habilite. Por estos motivos, le recomendamos que realice una de las siguientes acciones:

- Cambie el estado del flujo de trabajo de todos los hallazgos existentes a RESOLVED antes de deshabilitar Security Hub CSPM. Para obtener más información, consulte [Configuración del estado del flujo de trabajo de los hallazgos en Security Hub \(CSPM\)](#).
- Desactive todos los estándares al menos seis días antes de deshabilitar Security Hub CSPM. A continuación, Security Hub CSPM archiva todos los hallazgos existentes haciendo todo lo posible, normalmente en un plazo de tres a cinco días. Para obtener más información, consulte [Deshabilitación de un estándar de seguridad](#).

No puede deshabilitar el CSPM de Security Hub en los siguientes casos:

- Su cuenta es la cuenta de administrador de CSPM de Security Hub delegada para una organización. Si usa la configuración central, no puede asociar una política de configuración que deshabilite el CSPM de Security Hub para la cuenta de administrador delegado. La asociación puede realizarse correctamente para otras cuentas, pero Security Hub CSPM no aplica la política a la cuenta de administrador delegado.
- Su cuenta es una cuenta de administrador de CSPM de Security Hub por invitación y tiene cuentas de miembro. Antes de poder deshabilitar el CSPM de Security Hub, debe desasociar todas las cuentas de sus miembros. Para aprender a hacerlo, consulte [the section called “Desasociación de cuentas miembro”](#).

Para que el propietario de una cuenta de miembro pueda deshabilitar el CSPM de Security Hub, la cuenta debe desasociarse de su cuenta de administrador. En el caso de una cuenta de organización, solo la cuenta de administrador puede desasociar una cuenta de miembro. Para obtener más información, consulte [the section called “Desasociación de cuentas de la organización como cuentas de miembro”](#). En el caso de una cuenta invitada manualmente, la cuenta de administrador o la cuenta de miembro pueden desasociar la cuenta. Para obtener más información, consulte [the section called “Desasociación de cuentas miembro”](#) o [the section called “Desvinculación de una cuenta de administrador”](#). La desasociación no es necesaria si utiliza la configuración central, ya que el administrador del Security Hub CSPM puede crear una política que deshabilite el Security Hub CSPM para cuentas de miembros específicas.

Al deshabilitar el CSPM de Security Hub para una cuenta, solo se deshabilita en la cuenta actual. Región de AWS Sin embargo, si utilizas la configuración central para deshabilitar el CSPM de Security Hub para cuentas específicas, se deshabilitará en la región de origen y en todas las regiones vinculadas.

Para deshabilitar el CSPM de Security Hub, elija el método que prefiera y siga los pasos.

Security Hub CSPM console

Siga estos pasos para deshabilitar el CSPM de Security Hub mediante la consola.

Para deshabilitar Security Hub (CSPM)

1. Abra la consola AWS de Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, en Configuración, seleccione General.
3. En la sección Disable Security Hub CSPM, elija Disable Security Hub CSPM.
4. Cuando se te pida confirmación, selecciona Disable Security Hub CSPM.

Security Hub API

Para deshabilitar el CSPM de Security Hub mediante programación, utilice el [DisableSecurityHub](#) funcionamiento de la API de Security Hub AWS . O bien, si está utilizando el AWS CLI, ejecute el comando. [disable-security-hub](#) Por ejemplo, el siguiente comando desactiva el CSPM de Security Hub en la versión actual: Región de AWS

```
$ aws securityhub disable-security-hub
```


Seguridad en AWS Security Hub

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted 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 AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los [programas de conformidad de AWS](#). Para obtener más información sobre los programas de conformidad que se aplican a AWS Security Hub, consulte [Servicios de AWS en el ámbito del programa de conformidad](#).
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida al utilizar Security Hub. En los siguientes temas le mostramos cómo configurar Security Hub para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger los recursos de Security Hub.

Temas

- [Protección de datos en AWS Security Hub](#)
- [AWS Identity and Access Management para Security Hub](#)
- [Validación de la conformidad en AWS Security Hub](#)
- [Resiliencia en AWS Security Hub](#)
- [Seguridad de infraestructura en AWS Security Hub](#)
- [AWS Security Hub y puntos finales de VPC de interfaz \(AWS PrivateLink\)](#)

Protección de datos en AWS Security Hub

El modelo de [responsabilidad AWS compartida modelo](#) se aplica a la protección de datos en AWS Security Hub. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los 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, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios 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.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte [Cómo trabajar con CloudTrail senderos](#) en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados 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 por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final 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 cuando trabaja con Security Hub u otro Servicios de AWS dispositivo mediante la consola, la API o AWS SDKs. AWS CLI 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 información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Security Hub es una oferta de servicio para varios clientes. Para garantizar la protección de los datos, Security Hub cifra los datos en reposo y los datos en tránsito entre servicios de componentes.

AWS Identity and Access Management para Security Hub

AWS Identity and Access Management (IAM) es un sistema Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Security Hub. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [Cómo funciona Security Hub con IAM](#)
- [Ejemplos de políticas basadas en identidades de AWS Security Hub](#)
- [Funciones vinculadas al servicio para AWS Security Hub](#)
- [AWS políticas gestionadas para Security Hub](#)
- [Solución de problemas AWS Security Hub de identidad y acceso](#)

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que se realice en Security Hub.

Usuario de servicio: si utiliza el servicio de Security Hub para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Security Hub para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador.

Si no puede acceder a una característica en Security Hub, consulte [Solución de problemas AWS Security Hub de identidad y acceso](#).

Administrador de servicio: si está a cargo de los recursos de Security Hub en su empresa, probablemente tenga acceso completo a Security Hub. Es responsabilidad suya determinar a qué características y recursos de Security Hub deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestor de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Security Hub, consulte [Cómo funciona Security Hub con IAM](#).

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a Security Hub. Para consultar ejemplos de políticas basadas en identidades de Security Hub que puede utilizar en IAM, consulte [Ejemplos de políticas basadas en identidades de AWS Security Hub](#).

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestor habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte [Cómo iniciar sesión Cuenta de AWS en su](#) Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte [AWS Signature Versión 4 para solicitudes API](#) en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte [Autenticación multifactor](#) en la Guía del usuario de AWS IAM Identity Center y [Autenticación multifactor AWS en IAM](#) en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulta [¿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 propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como

contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte [Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración](#) en la Guía del usuario de IAM.

Un [grupo de IAM](#) es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdmins y concederle permisos para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. 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 dentro de su Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede [cambiar de un rol de usuario a uno de IAM](#) (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta [Métodos para asumir un rol](#) en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- **Acceso de usuario federado:** para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos que define el rol. Para obtener información acerca de roles de federación, consulte [Crear un rol para un proveedor de identidad de terceros \(federación\)](#) en la Guía del usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center.
- **Permisos de usuario de IAM temporales:** un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.

- **Acceso entre cuentas:** puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.
- **Acceso entre servicios:** algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
- **Sesiones de acceso directo (FAS):** cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Reenviar sesiones de acceso](#).
- **Rol de servicio:** un rol de servicio es un [rol de IAM](#) que adopta 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.
- **Función vinculada al servicio:** una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted 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.
- **Aplicaciones que se ejecutan en Amazon EC2:** puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene

el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte [Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon](#) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte [Información general de políticas JSON](#) en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

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.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS

administradas y políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, 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 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. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la [descripción general de la lista de control de acceso \(ACL\)](#) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- **Límites de permisos:** un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites

de los permisos, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del usuario de IAM.

- **Políticas de control de servicios (SCPs):** SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las [políticas de control de servicios](#) en la Guía del AWS Organizations usuario.
- **Políticas de control de recursos (RCPs):** RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte [Políticas de control de recursos \(RCPs\)](#) en la Guía del AWS Organizations usuario.
- **Políticas de sesión:** las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. 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 saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la [lógica de evaluación de políticas](#) en la Guía del usuario de IAM.

Cómo funciona Security Hub con IAM

Antes de usar AWS Identity and Access Management (IAM) para administrar el acceso AWS Security Hub, infórmese sobre las funciones de IAM disponibles para su uso con Security Hub.

Funciones de IAM que puede utilizar con AWS Security Hub

Característica de IAM	Soporte de Security Hub
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	No
Claves de condición de política	Sí
Listas de control de acceso () ACLs	No
Control de acceso basado en atributos (ABAC) – etiquetas en políticas	Sí
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo Servicios de AWS funcionan Security Hub y otras funciones con la mayoría de las funciones de IAM, consulte Servicios de AWS Cómo [funcionan con IAM](#) en la Guía del usuario de IAM.

Políticas basadas en identidad para Security Hub

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. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. 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.

Security Hub es compatible con las políticas basadas en identidad. Para obtener más información, consulte [Ejemplos de políticas basadas en identidades de AWS Security Hub](#).

Políticas basadas en recursos para Security Hub

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. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte [Cross account resource access in IAM](#) en la Guía del usuario de IAM.

Security Hub no admite políticas basadas en recursos. No puede adjuntar una política de IAM directamente a un recurso de Security Hub.

Acciones de la política para Security Hub

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON 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. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones de las políticas de Security Hub utilizan el siguiente prefijo antes de la acción:

```
securityhub:
```

Por ejemplo, para conceder a un usuario permiso para habilitar Security Hub, que es una acción que corresponde a la operación `EnableSecurityHub` de la API de Security Hub, debe incluir la acción `securityhub:EnableSecurityHub` en su política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. Security Hub define su propio conjunto de acciones que describen las tareas que se pueden realizar con este servicio.

```
"Action": "securityhub:EnableSecurityHub"
```

Para especificar varias acciones en una única instrucción, sepárelas con comas. Por ejemplo:

```
"Action": [  
    "securityhub:EnableSecurityHub",  
    "securityhub:BatchEnableStandards"
```

También puede utilizar caracteres comodín para especificar varias acciones (*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Get`, incluya la siguiente acción:

```
"Action": "securityhub:Get*"
```

Sin embargo, recomendamos que las políticas se creen según el principio de privilegios mínimos. En otras palabras, debe crear políticas que incluyan solo los permisos necesarios para realizar una tarea específica.

El usuario debe tener acceso a la operación `DescribeStandardsControl` para poder acceder a `BatchGetSecurityControls`, `BatchGetStandardsControlAssociations` y `ListStandardsControlAssociations`.

El usuario debe tener acceso a la operación `UpdateStandardsControls` para poder acceder a `BatchUpdateStandardsControlAssociations` y `UpdateSecurityControl`.

Para obtener una lista de las acciones de Security Hub, consulte [Acciones definidas por AWS Security Hub](#) en la Referencia de autorizaciones de servicio. Para ver ejemplos de políticas que especifican acciones de Security Hub, consulte [Ejemplos de políticas basadas en identidades de AWS Security Hub](#).

Recursos de políticas para Security Hub

Compatibilidad con recursos de políticas: no

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes 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. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el [Nombre de recurso de Amazon \(ARN\)](#). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"

```

Security Hub define los siguientes tipos de recursos:

- Hub
- Producto
- Agregador de resultados, también denominado agregador entre regiones
- Regla de automatización
- Configuración de políticas

Puede especificar estos tipos de recursos en las políticas mediante ARNs.

Para obtener una lista de los tipos de recursos de Security Hub y la sintaxis del ARN de cada uno, consulte [Tipos de recursos definidos por AWS Security Hub](#) en la Referencia de autorizaciones de servicio. Para saber qué acciones puede especificar para cada tipo de recurso, consulte [Acciones definidas por AWS Security Hub](#) en la Referencia de autorizaciones de servicio. Para ver ejemplos de políticas que especifican recursos, consulte [Ejemplos de políticas basadas en identidades de AWS Security Hub](#).

Claves de condición de política de Security Hub

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. 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.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación AND lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una OR operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta [Elementos de la política de IAM: variables y etiquetas](#) en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales en la Guía](#) del usuario de IAM.

Para obtener una lista de las claves de condición de Security Hub, consulte [Claves de condición para AWS Security Hub](#) en la Referencia de autorizaciones de servicio. Para obtener más información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte

[Acciones definidas por AWS Security Hub](#). Para ver ejemplos de políticas que utilizan claves de condición, consulte [Ejemplos de políticas basadas en identidades de AWS Security Hub](#).

Listas de control de acceso (ACLs) en Security Hub

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Security Hub no es compatible ACLs, lo que significa que no puede adjuntar una ACL a un recurso de Security Hub.

Control de acceso basado en atributos (ABAC) con Security Hub

Admite ABAC (etiquetas en las políticas): sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

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.

Puede adjuntar etiquetas a los recursos de Security Hub. También puede controlar el acceso a los recursos proporcionando información sobre las etiquetas en el elemento `Condition` de una política.

Para obtener información acerca del etiquetado de recursos de Security Hub, consulte [Etiquetado de los recursos de Security Hub \(CSPM\)](#). Para obtener un ejemplo de política basada en identidad que controla el acceso a un recurso basado en etiquetas, consulte [Ejemplos de políticas basadas en identidades de AWS Security Hub](#).

Uso de credenciales de seguridad temporales con Security Hub

Compatibilidad con credenciales temporales: sí

Algunos Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo [Servicios de AWS funcionan con IAM](#) en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte [Cambio de un usuario a un rol de IAM \(consola\)](#) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte [Credenciales de seguridad temporales en IAM](#).

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen llamando a operaciones de AWS STS API como [AssumeRole](#) o [GetFederationToken](#).

Security Hub admite el uso de credenciales temporales.

Sesiones de acceso directo en Security Hub

Admite sesiones de acceso directo (FAS): sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Reenviar sesiones de acceso](#).

Por ejemplo, Security Hub envía solicitudes de FAS a Downstream Servicios de AWS cuando se integra Security Hub AWS Organizations y cuando se designa la cuenta de administrador delegada del Security Hub para una organización en Organizations.

En lo que respecta a otras tareas, Security Hub permite al rol vinculado a un servicio llevar a cabo acciones en su nombre. Para obtener más información sobre este rol, consulte [Funciones vinculadas al servicio para AWS Security Hub](#).

Roles de servicios de Security Hub

Security Hub no asume ni utiliza roles de servicio. Security Hub utiliza un rol vinculado al servicio para llevar a cabo acciones en su nombre. Para obtener más información sobre este rol, consulte [Funciones vinculadas al servicio para AWS Security Hub](#).

Warning

El cambio de los permisos de un rol de servicio podría provocar problemas operativos con el uso de Security Hub. Edite los roles de servicio solo cuando Security Hub proporcione orientación para hacerlo.

Roles vinculados a servicios de Security Hub

Admite roles vinculados a servicios: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted 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.

Security Hub permite al rol vinculado a un servicio llevar a cabo acciones en su nombre. Para obtener más información sobre este rol, consulte [Funciones vinculadas al servicio para AWS Security Hub](#).

Ejemplos de políticas basadas en identidades de AWS Security Hub

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de Security Hub. Tampoco pueden realizar tareas mediante la AWS API, la AWS Management Console, el AWS CLI, o. Un administrador debe crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar operaciones de la API concretas en los recursos especificados que necesiten. El administrador debe adjuntar esas políticas a los usuarios o grupos que necesiten esos permisos.

Para obtener información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas JSON de ejemplo, consulte [Creación de políticas en la pestaña JSON](#) en la Guía del usuario de IAM.

Temas

- [Prácticas recomendadas relativas a políticas](#)
- [Cómo usar la consola de Security Hub](#)
- [Ejemplo: Permitir que los usuarios vean sus propios permisos](#)
- [Ejemplo: Permitir a los usuarios crear y administrar una política de configuración](#)
- [Ejemplo: Permitir a los usuarios ver los resultados](#)
- [Ejemplo: Permitir a los usuarios crear y administrar reglas de automatización](#)

Prácticas recomendadas relativas a políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Security Hub de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos en muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso.

Con el fin de obtener más información, consulta 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, consulta [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, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta [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.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para 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.

Cómo usar la consola de Security Hub

Para acceder a la AWS Security Hub consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Security Hub 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 concedas permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que esos usuarios y roles puedan usar la consola de Security Hub, adjunte también la siguiente política AWS administrada a la entidad. Para obtener más información, consulte [Agregar de permisos a un usuario](#) en la Guía del usuario de IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "securityhub.amazonaws.com"
        }
      }
    }
  ]
}
```

Ejemplo: Permitir que los usuarios vean sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas gestionadas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o 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": "*"
    }
]
}

```

Ejemplo: Permitir a los usuarios crear y administrar una política de configuración

En este ejemplo, se muestra cómo crear una política de IAM que permita a un usuario crear, ver, actualizar y eliminar políticas de configuración. En este ejemplo de política, también se permite al usuario iniciar, detener y ver asociaciones de políticas. Para que funcione esta política de IAM, el usuario debe ser el administrador delegado de Security Hub de la organización.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateConfigurationPolicy",
                "securityhub:UpdateConfigurationPolicy"
            ]
        }
    ]
}

```

```

    ],
    "Resource": "*"
  },
  {
    "Sid": "ViewConfigurationPolicy",
    "Effect": "Allow",
    "Action": [
      "securityhub:GetConfigurationPolicy",
      "securityhub:ListConfigurationPolicies"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DeleteConfigurationPolicy",
    "Effect": "Allow",
    "Action": [
      "securityhub:DeleteConfigurationPolicy"
    ],
    "Resource": "*"
  },
  {
    "Sid": "ViewConfigurationPolicyAssociation",
    "Effect": "Allow",
    "Action": [
      "securityhub:BatchGetConfigurationPolicyAssociations",
      "securityhub:GetConfigurationPolicyAssociation",
      "securityhub:ListConfigurationPolicyAssociations"
    ],
    "Resource": "*"
  },
  {
    "Sid": "UpdateConfigurationPolicyAssociation",
    "Effect": "Allow",
    "Action": [
      "securityhub:StartConfigurationPolicyAssociation",
      "securityhub:StartConfigurationPolicyDisassociation"
    ],
    "Resource": "*"
  }
]
}

```

Ejemplo: Permitir a los usuarios ver los resultados

En este ejemplo, se muestra cómo puede crear una política de IAM que permita a un usuario acceder a los resultados de Security Hub.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReviewFindings",
      "Effect": "Allow",
      "Action": [
        "securityhub:GetFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

Ejemplo: Permitir a los usuarios crear y administrar reglas de automatización

En este ejemplo, se muestra cómo puede crear una política de IAM que permita a un usuario crear, ver, actualizar y eliminar reglas de automatización de Security Hub. Para que funcione esta política de IAM, el usuario debe ser administrador de Security Hub. Para limitar los permisos (por ejemplo, para permitir que un usuario solo vea las reglas de automatización), puede eliminar los permisos de creación, actualización y eliminación.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateAndUpdateAutomationRules",
      "Effect": "Allow",
      "Action": [
        "securityhub:CreateAutomationRule",
        "securityhub:BatchUpdateAutomationRules"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ViewAutomationRules",
      "Effect": "Allow",
```



```
        "Action": [
            "securityhub:BatchGetAutomationRules",
            "securityhub:ListAutomationRules"
        ],
        "Resource": "*"
    },
    {
        "Sid": "DeleteAutomationRules",
        "Effect": "Allow",
        "Action": [
            "securityhub:BatchDeleteAutomationRules"
        ],
        "Resource": "*"
    }
]
```

Funciones vinculadas al servicio para AWS Security Hub

AWS Security Hub utiliza un rol vinculado a un [servicio AWS Identity and Access Management](#) (IAM) denominado `AWSServiceRoleForSecurityHub`. Este rol vinculado al servicio es un rol de IAM que está vinculado directamente a Security Hub. Está predefinido por Security Hub e incluye todos los permisos que Security Hub necesita para llamar a otros AWS recursos. Servicios de AWS y supervisarlos en su nombre. Security Hub utiliza esta función vinculada a un servicio en todos los lugares en los Regiones de AWS que Security Hub esté disponible.

Un rol vinculado a un servicio simplifica la configuración de Security Hub porque ya no tendrá que agregar de forma manual los permisos necesarios. Security Hub define los permisos de su rol vinculado a un servicio y, a menos que esté definido de otra manera, solo Security Hub puede asumir el rol. Los permisos definidos incluyen las políticas de confianza y de permisos, y no puede asociar esa política de permisos a ninguna otra entidad de IAM.

Para ver los detalles del rol vinculado a un servicio, en la página Configuración de la consola de Security Hub, seleccione General y, a continuación, Ver permisos del servicio.

Puede eliminar el rol vinculado a un servicio de Security Hub solo después de deshabilitar en primer lugar Security Hub en todas las regiones en las que se ha habilitado. De esta forma se protegen los recursos de Security Hub, ya que evita que se puedan eliminar accidentalmente permisos de acceso a estos recursos.

Para obtener información acerca de 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 tengan Sí en la columna Roles vinculados a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Temas

- [Permisos de roles vinculados a servicios de Security Hub](#)
- [Creación de un rol vinculado a un servicio de Security Hub](#)
- [Edición de un rol vinculado a un servicio de Security Hub](#)
- [Eliminación de un rol vinculado a un servicio de Security Hub](#)

Permisos de roles vinculados a servicios de Security Hub

Security Hub usa el rol vinculado a un servicio denominado `AWSServiceRoleForSecurityHub`. Es una función vinculada a un servicio necesaria para acceder AWS Security Hub a sus recursos. La función vinculada al servicio permite a Security Hub recibir las conclusiones de otros usuarios Servicios de AWS y configurar la AWS Config infraestructura necesaria para ejecutar las comprobaciones de seguridad de los controles.

El rol vinculado al servicio `AWSServiceRoleForSecurityHub` depende de los siguientes servicios para asumir el rol:

- `securityhub.amazonaws.com`

El rol vinculado al servicio `AWSServiceRoleForSecurityHub` utiliza la política administrada de [AWSSecurityHubServiceRolePolicy](#).

Debe conceder permisos para permitir a una identidad de IAM (como un rol, grupo o usuario) crear, editar o eliminar un rol vinculado a un servicio. Para que el rol vinculado al servicio `AWSServiceRoleForSecurityHub` se cree correctamente, la identidad de IAM que usa para acceder a Security Hub debe tener los permisos necesarios. Para conceder los permisos necesarios, adjunte la siguiente política a un rol, un grupo o un usuario.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
    "Action": "securityhub:*",
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "iam:AWSServiceName": "securityhub.amazonaws.com"
      }
    }
  }
]
```

Creación de un rol vinculado a un servicio de Security Hub

El rol vinculado al servicio `AWSServiceRoleForSecurityHub` se crea automáticamente cuando se habilita Security Hub por primera vez o al habilitar Security Hub en una región compatible en la que no estaba habilitado. También puede crear el rol vinculado al servicio `AWSServiceRoleForSecurityHub` manualmente con la consola de IAM, la CLI de IAM o la API de IAM.

Important

El rol vinculado al servicio creado para la cuenta de administrador de Security Hub no es aplicable a cuentas miembro de Security Hub.

Para obtener más información acerca de cómo crear un rol manualmente, consulte [Crear un rol vinculado a un servicio](#) en la Guía del usuario de IAM.

Edición de un rol vinculado a un servicio de Security Hub

Security Hub no le permite modificar el rol vinculado al servicio `AWSServiceRoleForSecurityHub`. 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 [Edición de un rol vinculado a un servicio](#) en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio de Security Hub

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, recomendamos que elimine dicho rol. De esta forma, no tendrá una entidad no utilizada cuya supervisión o mantenimiento no se realizan de forma activa.

Important

Para eliminar el rol vinculado al servicio `AWSServiceRoleForSecurityHub`, primero debe deshabilitar Security Hub en todas las regiones donde está habilitado.

Si Security Hub está habilitado cuando intenta eliminar el rol vinculado al servicio, el rol no se eliminará. Para obtener más información, consulte [Desactivación de Security Hub CSPM](#).

Cuando se deshabilita Security Hub, el rol vinculado al servicio `AWSServiceRoleForSecurityHub` no se deshabilita automáticamente. Si habilita Security Hub de nuevo, comienza a utilizar el rol vinculada al servicio `AWSServiceRoleForSecurityHub` existente.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la CLI de IAM o la API de IAM para eliminar el rol vinculado a servicios `AWSServiceRoleForSecurityHub`. Para obtener más información, consulte [Eliminación de un rol vinculado a un servicio](#) en la Guía del usuario de IAM.

AWS políticas gestionadas para Security Hub

Una política AWS administrada es una política independiente creada y administrada por AWS. Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir [políticas administradas por el cliente](#) específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte [Políticas administradas de AWS](#) en la Guía del usuario de IAM.

AWS política gestionada: AWSSecurityHubFullAccess

Puede adjuntar la política AWSSecurityHubFullAccess a las identidades de IAM.

Esta política concede permisos administrativos que permiten a un principal acceso completo a todas las acciones de CSPM de Security Hub. Esta política debe estar asociada a un director antes de que habilite el Security Hub CSPM manualmente para su cuenta. Por ejemplo, las entidades principales con estos permisos pueden tanto ver como actualizar el estado de los resultados. Pueden configurar información personalizada y habilitar integraciones. Pueden habilitar y deshabilitar estándares y controles. Las entidades principales de una cuenta de administrador también pueden administrar cuentas miembro.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- **securityhub**— Permite a los directores el acceso total a todas las acciones de CSPM de Security Hub.
- **guardduty**— Permite a los directores obtener información sobre el estado de las cuentas en Amazon GuardDuty.
- **iam**— Permite a los directores crear un rol vinculado a un servicio para Security Hub, CSPM y Security Hub.
- **inspector**: permite a las entidades principales obtener información acerca del estado de las cuentas de Amazon Inspector.
- **pricing**— Permite a los directores obtener una lista de precios y productos. Servicios de AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SecurityHubAllowAll",
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    }
  ]
}
```

```

    },
    {
      "Sid": "SecurityHubServiceLinkedRole",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": [
            "securityhub.amazonaws.com",
            "securityhubv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "OtherServicePermission",
      "Effect": "Allow",
      "Action": [
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "inspector2:BatchGetAccountStatus",
        "pricing:GetProducts"
      ],
      "Resource": "*"
    }
  ]
}

```

Política gestionada por CSPM de Security Hub: AWSSecurityHubReadOnlyAccess

Puede adjuntar la política `AWSSecurityHubReadOnlyAccess` a las identidades de IAM.

Esta política concede permisos de solo lectura que permiten a los usuarios ver la información en Security Hub CSPM. Los directores con esta política adjunta no pueden realizar ninguna actualización en Security Hub CSPM. Por ejemplo, las entidades principales con estos permisos pueden ver la lista de resultados asociados a su cuenta, pero no pueden cambiar el estado de un resultado. Pueden ver los resultados de las informaciones, pero no pueden crear ni configurar informaciones personalizadas. No pueden configurar controles ni integraciones de productos.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- **securityhub**: permite a los usuarios realizar acciones que devuelven una lista de elementos o detalles sobre un elemento. Esto incluye las operaciones de la API que comienzan con **Get**, **List** o **Describe**.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSSecurityHubReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "securityhub:Get*",
        "securityhub:List*",
        "securityhub:BatchGet*",
        "securityhub:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS política gestionada: AWSSecurityHubOrganizationsAccess

Puede adjuntar la política **AWSSecurityHubOrganizationsAccess** a las identidades de IAM.

Esta política otorga permisos administrativos para habilitar y administrar Security Hub y Security Hub CSPM dentro de una organización.

Los permisos de esta política permiten a la cuenta de administración de la organización designar la cuenta de administrador delegado para Security Hub y Security Hub CSPM. También permiten que la cuenta de administrador delegado habilite las cuentas de la organización como cuentas de miembros.

Esta política solo proporciona los permisos a Organizations. La cuenta de administración de la organización y la cuenta de administrador delegado también requieren permisos para las acciones asociadas. Estos permisos se pueden conceder mediante la política administrada de **AWSSecurityHubFullAccess**.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `organizations:ListAccounts`: permite a las entidades principales recuperar la lista de cuentas que pertenecen a una organización.
- `organizations:DescribeOrganization`: permite a las entidades principales recuperar información sobre la organización.
- `organizations:ListRoots`: permite a las entidades principales enumerar la raíz de una organización.
- `organizations:ListDelegatedAdministrators`: permite a las entidades principales enumerar el administrador delegado de una organización.
- `organizations:ListAWSServiceAccessForOrganization`— Permite a los directores enumerar los Servicios de AWS que usa una organización.
- `organizations:ListOrganizationalUnitsForParent`: permite a las entidades principales enumerar las unidades organizativas (OU) secundarias de una unidad organizativa principal.
- `organizations:ListAccountsForParent`: permite a las entidades principales enumerar las cuentas secundarias de una unidad organizativa principal.
- `organizations:ListParents`— Muestra la raíz o las unidades organizativas (OUs) que actúan como matrices inmediatas de la unidad organizativa o cuenta secundaria especificada.
- `organizations:DescribeAccount`: permite a las entidades principales recuperar información de sobre una cuenta en una organización.
- `organizations:DescribeOrganizationalUnit`: permite a las entidades principales recuperar información sobre una unidad organizativa de la organización.
- `organizations:ListPolicies`— Recupera la lista de todas las políticas de una organización de un tipo específico.
- `organizations:ListPoliciesForTarget`— Muestra las políticas que están directamente asociadas a la raíz, unidad organizativa (OU) o cuenta de destino especificadas.
- `organizations:ListTargetsForPolicy`— Muestra todas las raíces, unidades organizativas (OUs) y cuentas a las que está asociada la política especificada.
- `organizations:EnableAWSServiceAccess`— Permite a los directores habilitar la integración con Organizations.
- `organizations:RegisterDelegatedAdministrator`— Permite a los directores designar la cuenta de administrador delegado.
- `organizations:DeregisterDelegatedAdministrator`— Permite a los directores eliminar la cuenta de administrador delegado.
- `organizations:DescribePolicy`— Recupera información sobre una política.

- `organizations:DescribeEffectivePolicy`— Devuelve el contenido de la política vigente para el tipo de póliza y la cuenta especificados.
- `organizations:CreatePolicy`— Crea una política de un tipo específico que se puede adjuntar a una cuenta raíz, a una unidad organizativa (OU) o a una AWS cuenta individual.
- `organizations:UpdatePolicy`— Actualiza una política existente con un nombre, descripción o contenido nuevos.
- `organizations>DeletePolicy`— Elimina la política especificada de su organización.
- `organizations:AttachPolicy`— Adjunta una política a una cuenta raíz, a una unidad organizativa (OU) o a una cuenta individual.
- `organizations:DetachPolicy`— Separa una política de una raíz, unidad organizativa (OU) o cuenta de destino.
- `organizations:EnablePolicyType`— Habilita un tipo de política en una raíz.
- `organizations:DisablePolicyType`— Desactiva un tipo de política organizacional en una raíz.
- `organizations:TagResource`— Añade una o más etiquetas al recurso especificado.
- `organizations:UntagResource`— Elimina cualquier etiqueta con las claves especificadas del recurso especificado.
- `organizations:ListTagsForResource`— Muestra las etiquetas adjuntas al recurso especificado.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OrganizationPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:DescribeAccount",

```

```

        "organizations:DescribeOrganizationalUnit",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy"
    ],
    "Resource": "*"
},
{
    "Sid": "OrganizationPermissionsEnable",
    "Effect": "Allow",
    "Action": "organizations:EnableAWSServiceAccess",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal": "securityhub.amazonaws.com"
        }
    }
},
{
    "Sid": "OrganizationPermissionsDelegatedAdmin",
    "Effect": "Allow",
    "Action": [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
    ],
    "Resource": "arn:aws:organizations::*:account/o-*/*",
    "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal": "securityhub.amazonaws.com"
        }
    }
},
{
    "Sid": "OrganizationPolicyPermissions",
    "Effect": "Allow",
    "Action": [
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations>DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",

```

```

        "organizations:DisablePolicyType"
    ],
    "Resource": [
        "arn:aws:organizations:::root/o-*/**",
        "arn:aws:organizations:::account/o-*/**",
        "arn:aws:organizations:::ou/o-*/**",
        "arn:aws:organizations:::policy/o-*/securityhub_policy/*"
    ],
    "Condition": {
        "StringLikeIfExists": {
            "organizations:PolicyType": "SECURITYHUB_POLICY"
        }
    }
},
{
    "Sid": "OrganizationPolicyTaggingPermissions",
    "Effect": "Allow",
    "Action": [
        "organizations:TagResource",
        "organizations:UntagResource",
        "organizations:ListTagsForResource"
    ],
    "Resource": [
        "arn:aws:organizations:::policy/o-*/securityhub_policy/*"
    ]
}
]
}

```

AWS política gestionada: AWSSecurityHubServiceRolePolicy

No puede asociar AWSSecurityHubServiceRolePolicy a sus entidades IAM. Esta política se adjunta a un rol vinculado a un servicio que permite a Security Hub CSPM realizar acciones en su nombre. Para obtener más información, consulte [the section called “Roles vinculados a servicios”](#).

Esta política concede permisos administrativos que permiten al rol vinculado al servicio realizar las comprobaciones de seguridad de los controles CSPM de Security Hub.

Detalles de los permisos

Esta política incluye permisos para hacer lo siguiente:

- `cloudtrail`— Recuperar información sobre los senderos. CloudTrail

- **cloudwatch**— Recupera las CloudWatch alarmas actuales.
- **logs**— Recupera los filtros métricos para CloudWatch los registros.
- **sns**: recuperar la lista de suscripciones a un tema de SNS.
- **config**— Recuperar información sobre los registradores de configuración, los recursos y AWS Config las reglas. También permite que el rol vinculado a un servicio cree y elimine reglas de AWS Config y ejecute evaluaciones en función de las reglas.
- **iam**: obtener y generar informes de credenciales de cuentas.
- **organizations**: recuperar información de cuentas y unidades organizativas (OU) de una organización.
- **securityhub**— Recupere información sobre cómo se configuran el servicio, los estándares y los controles CSPM de Security Hub.
- **tag**: recuperar información sobre las etiquetas de recursos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SecurityHubServiceRolePermissions",
      "Effect": "Allow",
      "Action": [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "logs:DescribeMetricFilters",
        "sns:ListSubscriptionsByTopic",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",
        "iam:GenerateCredentialReport",
        "organizations:ListAccounts",
        "config:PutEvaluations",
        "tag:GetResources",
        "iam:GetCredentialReport",
        "organizations:DescribeAccount",
```

```

        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "securityhub:BatchDisableStandards",
        "securityhub:BatchEnableStandards",
        "securityhub:BatchUpdateStandardsControlAssociations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:CreateMembers",
        "securityhub>DeleteMembers",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandards",
        "securityhub:DescribeStandardsControls",
        "securityhub:DisassociateFromAdministratorAccount",
        "securityhub:DisassociateMembers",
        "securityhub:DisableSecurityHub",
        "securityhub:EnableSecurityHub",
        "securityhub:GetEnabledStandards",
        "securityhub:ListStandardsControlAssociations",
        "securityhub:ListSecurityControlDefinitions",
        "securityhub:UpdateOrganizationConfiguration",
        "securityhub:UpdateSecurityControl",
        "securityhub:UpdateSecurityHubConfiguration",
        "securityhub:UpdateStandardsControl",
        "tag:GetResources"
    ],
    "Resource": "*"
},
{
    "Sid": "SecurityHubServiceRoleConfigPermissions",
    "Effect": "Allow",
    "Action": [
        "config:PutConfigRule",
        "config>DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule"
    ],
    "Resource": "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
},
{
    "Sid": "SecurityHubServiceRoleOrganizationsPermissions",
    "Effect": "Allow",
    "Action": [

```

```
        "organizations:ListDelegatedAdministrators"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal": [
                "securityhub.amazonaws.com"
            ]
        }
    }
}
]
```

AWS política gestionada: AWSSecurityHubV2ServiceRolePolicy

Note

Security Hub está en versión preliminar y está sujeto a cambios.

Esta política permite a Security Hub gestionar AWS Config las reglas y los recursos del Security Hub en su organización y en su nombre. Esta política está asociada a un rol vinculado a un servicio. Esto permite a dicho servicio realizar acciones por usted. No puede asociar esta política a los usuarios, grupos o roles. Para obtener más información, consulte [the section called “Roles vinculados a servicios”](#).

Detalles de los permisos

Esta política incluye permisos para hacer lo siguiente:

- **config**— Administra los grabadores de configuración vinculados a servicios para los recursos de Security Hub.
- **iam**— Crea el rol vinculado al servicio para. AWS Config
- **organizations**— Recupera la información de la cuenta y la unidad organizativa (OU) de una organización.
- **securityhub**— Administra la configuración del Security Hub.
- **tag**— Recupera información sobre las etiquetas de recursos.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SecurityHubV2ServiceRoleAssetsConfig",
      "Effect": "Allow",
      "Action": [
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutServiceLinkedConfigurationRecorder"
      ],
      "Resource": "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForSecurityHubAssets/*"
    },
    {
      "Sid": "SecurityHubV2ServiceRoleAssetsIamPermissions",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam:*:*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "config.amazonaws.com"
        }
      }
    },
    {
      "Sid": "SecurityHubV2ServiceRoleSecurityHubPermissions",
      "Effect": "Allow",
      "Action": [
        "securityhub:DisableSecurityHubV2",
        "securityhub:EnableSecurityHubV2",
        "securityhub:DescribeSecurityHubV2"
      ],
      "Resource": "arn:aws:securityhub:*:*:hubv2/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}

```

```

    },
    {
      "Sid": "SecurityHubV2ServiceRoleTagPermissions",
      "Effect": "Allow",
      "Action": [
        "tag:GetResources"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SecurityHubV2ServiceRoleOrganizationsPermissionsOnResources",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource": "arn:aws:organizations::*:*"
    },
    {
      "Sid": "SecurityHubV2ServiceRoleOrganizationsPermissionsWithoutResources",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SecurityHubV2ServiceRoleDelegatedAdminPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  }
}

```



```
]
}
```

Security Hub CSPM actualiza las políticas gestionadas AWS

Vea los detalles sobre las actualizaciones de las políticas AWS administradas para Security Hub CSPM desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página de [historial de documentos](#) CSPM de Security Hub.

Cambio	Descripción	Fecha
AWSSecurityHubOrganizationsAccess : actualización de una política actual	Security Hub CSPM agregó un nuevo permiso a. <code>AWSSecurityHubOrganizationsAccess</code> El permiso permite a la administración de la organización habilitar y administrar Security Hub y Security Hub CSPM dentro de una organización.	17 de junio de 2025
AWSSecurityHubOrganizationsAccess : actualización de una política actual	Se agregaron nuevos permisos que permiten a la administración de la organización habilitar y administrar Security Hub y Security Hub CSPM dentro de una organización.	17 de junio de 2025
AWSSecurityHubFullAccess : actualización de una política actual	Security Hub CSPM agregó un nuevo permiso que permite a los directores crear un rol vinculado a un servicio para Security Hub.	17 de junio de 2025

Cambio	Descripción	Fecha
AWSSecurityHUBv2ServiceRolePolicy : nueva política	Security Hub agregó una nueva política para permitir que Security Hub administre AWS Config las reglas y los recursos del Security Hub en la organización de un cliente y en su nombre. Security Hub está en versión preliminar y está sujeto a cambios.	17 de junio de 2025
AWSSecurityHubFullAccess — Actualización de una política existente	Security Hub CSPM actualizó la política para obtener información detallada sobre los precios Servicios de AWS y los productos.	24 de abril de 2024
AWSSecurityHubReadOnlyAccess — Actualización de una política existente	Security Hub CSPM actualizó esta política gestionada añadiendo un Sid campo.	22 de febrero de 2024
AWSSecurityHubFullAccess — Actualización a una política existente	Security Hub CSPM actualizó la política para determinar si Amazon GuardDuty y Amazon Inspector están habilitados en una cuenta. Esto ayuda a los clientes a reunir información relacionada con la seguridad de múltiples fuentes. Servicios de AWS	16 de noviembre de 2023

Cambio	Descripción	Fecha
AWSSecurityHubOrganizationsAccess — Actualización a una política existente	Security Hub CSPM actualizó la política para conceder permisos adicionales que permitieran el acceso de solo lectura a la funcionalidad de administrador delegado. AWS Organizations Esto incluye detalles como la raíz, las unidades organizativas (OUs), las cuentas, la estructura organizativa y el acceso a los servicios.	16 de noviembre de 2023
AWSSecurityHubServiceRolePolicy : actualización de una política actual	Security Hub CSPM agregó BatchGetSecurityControls DisassociateFromAdministratorAccount , y UpdateSecurityControl permisos para leer y actualizar las propiedades de control de seguridad personalizables.	26 de noviembre de 2023
AWSSecurityHubServiceRolePolicy : actualización de una política actual	Security Hub CSPM agregó el tag: GetResources permiso para leer las etiquetas de recursos relacionadas con los hallazgos.	7 de noviembre de 2023

Cambio	Descripción	Fecha
AWSSecurityHubServiceRolePolicy : actualización de una política actual	Security Hub CSPM agregó el <code>BatchGetStandardsControlAssociations</code> permiso para obtener información sobre el estado de habilitación de un control en un estándar.	27 de septiembre de 2023
AWSSecurityHubServiceRolePolicy : actualización de una política actual	El Security Hub CSPM agregó nuevos permisos para obtener AWS Organizations datos y leer y actualizar las configuraciones del Security Hub CSPM, incluidos los estándares y los controles.	20 de septiembre de 2023
AWSSecurityHubServiceRolePolicy : actualización de una política actual	Security Hub CSPM trasladó el <code>config:DescribeConfigRuleEvaluationStatus</code> permiso existente a una declaración diferente dentro de la política. El permiso <code>config:DescribeConfigRuleEvaluationStatus</code> se aplica ahora a todos los recursos.	17 de marzo de 2023

Cambio	Descripción	Fecha
AWSSecurityHubServiceRolePolicy : actualización de una política actual	Security Hub CSPM trasladó el <code>config:PutEvaluations</code> permiso existente a una declaración diferente dentro de la política. El permiso <code>config:PutEvaluations</code> se aplica ahora a todos los recursos.	14 de julio de 2021
AWSSecurityHubServiceRolePolicy : actualización de una política actual	Security Hub CSPM agregó un nuevo permiso para permitir que la función vinculada al servicio entregue los resultados de la evaluación. AWS Config	29 de junio de 2021
AWSSecurityHubServiceRolePolicy — Se agregó a la lista de políticas administradas	Se agregó información sobre la política administrada <code>AWSSecurityHubServiceRolePolicy</code> , que utiliza el rol vinculado al servicio CSPM de Security Hub.	11 de junio de 2021
AWSSecurityHubOrganizationsAccess — Nueva política	Security Hub CSPM agregó una nueva política que otorga los permisos necesarios para la integración de Security Hub CSPM con las organizaciones.	15 de marzo de 2021
Security Hub CSPM comenzó a rastrear los cambios	Security Hub CSPM comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	15 de marzo de 2021

Solución de problemas AWS Security Hub de identidad y acceso

Utilice la siguiente información para ayudarle a diagnosticar y solucionar problemas comunes que pueden surgir al trabajar con un AWS Security Hub IAM.

Temas

- [No tengo autorización para realizar una acción en Security Hub](#)
- [No estoy autorizado a realizar iam: PassRole](#)
- [Quiero tener acceso programático a Security Hub](#)
- [Soy administrador y deseo permitir que otros obtengan acceso a Security Hub](#)
- [Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a los recursos de mi Security Hub](#)

No tengo autorización para realizar una acción en Security Hub

Si AWS Management Console le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. El gestor es la persona que le proporcionó las credenciales de inicio de sesión.

El siguiente ejemplo de error se produce cuando el usuario mateojackson intenta usar la consola para ver los detalles de una *widget*, pero no tiene `securityhub:GetWidget` permisos.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
securityhub:GetWidget on resource: my-example-widget
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso *my-example-widget* mediante la acción `securityhub:GetWidget`.

No estoy autorizado a realizar iam: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a Security Hub.

Algunos Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un 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 realizar una acción en Security Hub. 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 administrador. AWS El gestor es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero tener acceso programático a Security Hub

Los usuarios necesitan acceso programático si quieren interactuar con personas AWS ajenas a. AWS Management Console La forma de conceder el acceso programático depende del tipo de usuario que acceda. AWS

Para conceder acceso programático a los usuarios, elija una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	Mediante
Identidad del personal (Usuarios administrados en el IAM Identity Center)	Usa credenciales temporales para firmar las solicitudes programáticas dirigidas al AWS CLI AWS SDKs, o. AWS APIs	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Configuración del AWS CLI uso AWS IAM Identity Center en la Guía del AWS Command Line Interface usuario. • Para AWS SDKs ver las herramientas y AWS APIs, consulte la autenticación del Centro de Identidad de IAM en la Guía de referencia de

¿Qué usuario necesita acceso programático?	Para	Mediante
		herramientas AWS SDKs y herramientas.
IAM	Utilice credenciales temporales para firmar las solicitudes programáticas dirigidas al AWS CLI AWS SDKs, o. AWS APIs	Siga las instrucciones de Uso de credenciales temporales con AWS recursos de la Guía del usuario de IAM.
IAM	(No recomendado) Utilice credenciales de larga duración para firmar las solicitudes programáticas dirigidas al AWS CLI AWS SDKs, o. AWS APIs	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Autenticación con credenciales de usuario de IAM en la Guía del AWS Command Line Interface usuario. • Para obtener AWS SDKs información sobre las herramientas, consulte Autenticarse con credenciales de larga duración en la Guía de referencia de herramientas AWS SDKs y herramientas. • Para ello AWS APIs, consulte Administrar las claves de acceso para los usuarios de IAM en la Guía del usuario de IAM.

Soy administrador y deseo permitir que otros obtengan acceso a Security Hub

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

Cree un conjunto de permisos. Siga las instrucciones de [Creación de un conjunto de permisos](#) en la Guía del usuario de AWS IAM Identity Center .

- Usuarios gestionados en IAM a través de un proveedor de identidades:

Cree un rol para la federación de identidades. Siga las instrucciones descritas en [Creación de un rol para un proveedor de identidad de terceros \(federación\)](#) en la Guía del usuario de IAM.

- Usuarios de IAM:

- Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en [Creación de un rol para un usuario de IAM](#) en la Guía del usuario de IAM.
- (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en [Adición de permisos a un usuario \(consola\)](#) de la Guía del usuario de IAM.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a los recursos de mi Security Hub

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 admiten políticas basadas en recursos o listas de control de acceso (ACLs), puede usar esas políticas para permitir que las personas accedan a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información sobre la compatibilidad de Security Hub con estas características, consulte [Cómo funciona Security Hub con IAM](#).
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte [Proporcionar acceso a un usuario de IAM en otro de su propiedad en la Cuenta de AWS Guía del usuario](#) de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta [Cómo proporcionar acceso a recursos que Cuentas de AWS 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 en AWS Security Hub

Para saber si un Servicio de AWS está incluido en el ámbito de programas de conformidad específicos, consulte [Servicios de AWS en el ámbito del programa de conformidad Servicios de AWS](#) y escoja el programa de conformidad que le interese. Para obtener información general, consulte Programas de [AWS cumplimiento > Programas 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 utilizarlos 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. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- [Cumplimiento de seguridad y gobernanza](#): en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- [Referencia de servicios válidos de HIPAA](#): muestra una lista con los servicios válidos de HIPAA. No todos los Servicios de AWS son aptos para HIPAA.
- [AWS Recursos](#) de de conformidad de: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- [AWS Guías de cumplimiento para clientes](#) de: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las prácticas recomendadas para garantizar la seguridad de los Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología [NIST], el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago [PCI] y la Organización Internacional de Normalización [ISO]).

- [Evaluación de recursos con reglas](#) en la Guía para AWS Config desarrolladores de: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normativas.
- [AWS Security Hub](#)— Este Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la [Referencia de controles de Security Hub](#).
- [Amazon GuardDuty](#): este Servicio de AWS detecta posibles amenazas para sus Cuentas de AWS, cargas de tarea, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a satisfacer varios requisitos de conformidad, como PCI DSS, cumpliendo los requisitos de detección de intrusos que exigen determinados marcos de conformidad.
- [AWS Audit Manager](#): este le Servicio de AWS ayuda a auditar continuamente el AWS uso de con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

Resiliencia en AWS Security Hub

La infraestructura AWS global se basa en dos zonas Regiones de AWS de disponibilidad. 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 demora. 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 uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte [Infraestructura AWS global](#).

Seguridad de infraestructura en AWS Security Hub

Como servicio gestionado, AWS Security Hub está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte [Seguridad AWS en la nube](#). Para diseñar su AWS entorno utilizando las

mejores prácticas de seguridad de la infraestructura, consulte [Protección de infraestructuras en un marco](#) de buena AWS arquitectura basado en el pilar de la seguridad.

Las llamadas a la API AWS publicadas se utilizan para acceder a Security Hub 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.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

AWS Security Hub y puntos finales de VPC de interfaz ()AWS PrivateLink

Puede establecer una conexión privada entre la VPC y AWS Security Hub mediante la creación de un punto de conexión de VPC de interfaz. Los puntos de conexión de interfaz cuentan con tecnología de que le permite acceder de forma privada a Security Hub APIs sin una puerta de enlace de Internet, un dispositivo NAT, una conexión de VPN o una conexión de AWS Direct Connect. [AWS PrivateLink](#) Las instancias de la VPC no necesitan direcciones IP públicas para comunicarse con Security Hub. APIs El tráfico entre la VPC y Security Hub 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 [Acceso y Servicio de AWS uso de un punto final de VPC de interfaz](#) en la Guía Amazon Virtual Private Cloud.

Consideraciones para los puntos de conexión de VPC de Security Hub

Antes de configurar un punto de conexión de VPC de interfaz para Security Hub, revise los requisitos previos y demás información de la Guía de [Amazon Virtual Private](#) Hub.

Security Hub admite la realización de llamadas a todas las acciones de la API desde su VPC.

Creación de un punto de conexión de VPC de la interfaz para Security Hub

Puede crear un punto de conexión de VPC para el servicio de Security Hub mediante la consola de Amazon VPC o (). AWS Command Line Interface AWS CLI Para obtener más información, consulte [Crear un punto de enlace de VPC](#) en la Guía Amazon Virtual Private Cloud.

Cree un punto de conexión de VPC para Security Hub mediante el siguiente nombre de servicio:

`com.amazonaws.region.securityhub`

¿Dónde *region* está el código de región del correspondiente? Región de AWS

Si habilita un DNS privado para el punto de conexión, podrá realizar solicitudes de API a Security Hub mediante el uso del nombre de DNS predeterminado de la región, por `securityhub.us-east-1.amazonaws.com` ejemplo, EE. UU. Este (Norte de Virginia).

Creación de una política de punto de conexión de VPC para Security Hub

Puede adjuntar una política de punto de conexión al punto de conexión de VPC que controla el acceso a Security Hub. 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 [Controlar el acceso a los puntos de enlace de la VPC mediante políticas de puntos de conexión](#) en la Guía de Amazon Virtual Private Cloud.

Ejemplo: política de punto de conexión de VPC para acciones de Security Hub

El siguiente es un ejemplo de un resultado típico de una política de punto de conexión para Security Hub. Cuando se asocia con un punto de conexión, esta política concede acceso a las acciones de Security Hub mostradas para todas las entidades principales en todos los recursos.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
```

```
        "securityhub:getFindings",
        "securityhub:getEnabledStandards",
        "securityhub:getInsights"
    ],
    "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 sus subredes de VPC con otras cuentas en la Guía Amazon Virtual Private Cloud](#).

Registro de llamadas a la API CSPM de Security Hub con CloudTrail

AWS Security Hub Cloud Security Posture Management (CSPM) está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Security Hub CSPM. CloudTrail captura las llamadas a la API para Security Hub CSPM como eventos. Las llamadas capturadas incluyen llamadas desde la consola CSPM de Security Hub y llamadas de código a las operaciones de la API CSPM de Security Hub. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para Security Hub CSPM. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información que CloudTrail recopila, puede determinar la solicitud que se realizó a Security Hub CSPM, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, incluido cómo configurarlo y habilitarlo, consulte la Guía del [AWS CloudTrail usuario](#).

Información sobre CSPM de Security Hub en CloudTrail

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad de eventos admitida en Security Hub CSPM, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los últimos eventos de su cuenta. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail eventos](#).

Para obtener un registro continuo de los eventos de su cuenta, incluidos los eventos de Security Hub CSPM, cree un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, este se aplica a todas las regiones de AWS . La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- [Introducción a la creación de registros de seguimiento](#)
- [CloudTrail servicios e integraciones compatibles](#)

- [Configuración de las notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

El CSPM de Security Hub admite el registro de todas las acciones de la API CSPM de Security Hub como eventos en los registros. CloudTrail Para ver una lista de las operaciones de CSPM de Security Hub, consulte la referencia de la API de [CSPM de Security Hub](#).

Cuando se registra la actividad de las siguientes acciones CloudTrail, el valor de `responseElements` es `null`. Esto garantiza que la información confidencial no se incluya en CloudTrail los registros.

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

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 realizó con credenciales de usuario root o AWS Identity and Access Management (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 AWS

Para obtener más información, consulte el [elemento `userIdentity` de CloudTrail](#).

Ejemplo: entradas del archivo de registro CSPM de Security Hub

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud,

etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la CreateInsight acción. En este ejemplo, se crea una información llamada Test Insight. Se especifica el atributo ResourceId como el agregador Agrupar por y no se especifican filtros opcionales para esta información. Para obtener más información acerca de las informaciones, consulte [Visualización de información en Security Hub CSPM](#).

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAJK6U5DS22IAVUI7BW",
    "arn": "arn:aws:iam::012345678901:user/TestUser",
    "accountId": "012345678901",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "TestUser"
  },
  "eventTime": "2018-11-25T01:02:18Z",
  "eventSource": "securityhub.amazonaws.com",
  "eventName": "CreateInsight",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "205.251.233.179",
  "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
  "requestParameters": {
    "Filters": {},
    "ResultField": "ResourceId",
    "Name": "Test Insight"
  },
  "responseElements": {
    "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
  },
  "requestID": "c0ffffccd-f04d-11e8-93fc-ddcd14710066",
  "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "012345678901"
}
```

Etiquetado de los recursos de Security Hub (CSPM)

Una etiqueta es una etiqueta opcional que puede definir y asignar a AWS los recursos, incluidos determinados tipos de recursos de AWS Security Hub Cloud Security Posture Management (CSPM). Las etiquetas pueden ayudarle a identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Por ejemplo, puede usar etiquetas para distinguir entre los recursos, identificar recursos que admiten ciertos requisitos de conformidad o flujos de trabajo, o asignar costos.

Puede añadir etiquetas a los siguientes tipos de recursos CSPM de Security Hub:

- Reglas de automatización
- Políticas de configuración
- Recurso de Hub

Conceptos básicos del etiquetado

Un recurso puede tener hasta 50 etiquetas. Cada etiqueta está formada por una clave de etiqueta y un valor de etiqueta opcional, ambos definidos por el usuario. Un clave de etiqueta es una etiqueta general que actúa como una categoría para un valor de etiqueta más específicos. Un valor de etiqueta actúa como descriptor de una clave de etiqueta.

Por ejemplo, si crea reglas de automatización diferentes para entornos diferentes (un conjunto de reglas de automatización para las cuentas de prueba y otro para las cuentas de producción), puede asignar una clave de etiqueta `Environment` a esas reglas. El valor de etiqueta asociado puede ser `Test` para las reglas asociadas a las cuentas de prueba y `Prod` para las reglas asociadas a las cuentas de producción y. OUs

Al definir y asignar etiquetas a los recursos de AWS Security Hub Cloud Security Posture Management (CSPM), tenga en cuenta lo siguiente:

- Cada recurso puede tener un máximo de 50 etiquetas.
- Para cada recurso, cada clave de etiqueta debe ser única y solo puede tener un valor.
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Le recomendamos que defina una estrategia de uso de mayúsculas y minúsculas en las etiquetas e implemente esa estrategia sistemáticamente en todos los recursos.

- Una clave de etiqueta puede tener un máximo de 128 caracteres UTF-8. Una clave de valor puede tener un máximo de 256 caracteres UTF-8. Los caracteres pueden ser letras, números, espacios o los siguientes símbolos: `_ . : / = + - @`
- El `aws :` prefijo está reservado para su uso por parte de AWS. No puede usarlo en las claves o valores de etiqueta que defina. Además, las claves o valores de etiqueta que utilizan este prefijo no se pueden cambiar ni quitar. Las etiquetas que usan este prefijo no cuentan para la cuota de 50 etiquetas por recurso.
- Las etiquetas que asigne estarán disponibles solo para usted Cuenta de AWS y solo en el lugar Región de AWS en el que las asigne.
- Si asigna etiquetas a un recurso mediante Security Hub CSPM, las etiquetas se aplican solo al recurso que está almacenado directamente en Security Hub CSPM, en el caso correspondiente. Región de AWS No se aplican a ningún recurso de soporte asociado que Security Hub CSPM cree, utilice o mantenga para usted en otros. Servicios de AWS Por ejemplo, si asigna etiquetas a una regla de automatización que actualiza los resultados relacionados con Amazon Simple Storage Service (Amazon S3), las etiquetas se aplican únicamente a su regla de automatización en Security Hub (CSPM) para la región especificada. No se aplican a sus buckets de S3. Para asignar también etiquetas a un recurso asociado, puede usar AWS Resource Groups o el Servicio de AWS que almacena el recurso, por ejemplo, Amazon S3 para un bucket de S3. La asignación de etiquetas a los recursos asociados puede ayudarle a identificar los recursos de apoyo para los recursos de CSPM de Security Hub.
- Si elimina un recurso, también se eliminará cualquier etiqueta asignada a dicho recurso.

 Important

No almacene datos confidenciales ni de otro tipo en etiquetas. Se puede acceder a las etiquetas desde muchos Servicios de AWS, entre ellos. Administración de facturación y costos de AWS No se diseñaron para utilizarse con datos confidenciales.

Para agregar y administrar etiquetas para los recursos CSPM de Security Hub, puede usar la consola CSPM de Security Hub, la API CSPM de Security Hub o la API de etiquetado. AWS Resource Groups Con Security Hub CSPM, puede añadir etiquetas a un recurso al crearlo. También puede añadir y gestionar etiquetas para los recursos individuales existentes. Con Resource Groups, puede añadir y administrar etiquetas de forma masiva para varios recursos existentes que abarquen varios Servicios de AWS, incluido Security Hub CSPM.

Para obtener consejos y prácticas recomendadas adicionales sobre el etiquetado, consulte [Etiquetar los recursos en la Guía del usuario sobre cómo etiquetar AWS los recursos](#). AWS

Uso de etiquetas en políticas de IAM

Una vez que comience a etiquetar los recursos, puede definir permisos de recursos basados en etiquetas en las políticas de AWS Identity and Access Management (IAM). Al utilizar las etiquetas de este modo, puede implementar un control pormenorizado sobre qué usuarios y roles de su empresa Cuenta de AWS tienen permiso para crear y etiquetar recursos, y qué usuarios y roles tienen permiso para añadir, editar y eliminar etiquetas de forma más general. Para controlar el acceso basándose función de etiquetas, puede utilizar [claves de condición relacionadas con las etiquetas](#) en el [elemento Condition](#) de las políticas de IAM.

Por ejemplo, puede crear una política de IAM que permita a un usuario tener acceso total a todos los recursos de AWS Security Hub Cloud Security Posture Management (CSPM), si la Owner etiqueta del recurso especifica su nombre de usuario:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ModifyResourceIfOwner",
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
      }
    }
  ]
}
```

Si define los permisos de nivel de recurso basados en etiquetas, estos entrarán en vigor inmediatamente. Esto significa que sus recursos están más seguros en cuanto se crean y que puede empezar a aplicar el uso de etiquetas de nuevos recursos rápidamente. También puede usar permisos de nivel de recurso para controlar las claves y valores de etiqueta que se pueden asociar a recursos nuevos y existentes. Para obtener más información, consulte [Controlar el acceso a AWS los recursos mediante etiquetas](#) en la Guía del usuario de IAM.

Añadir etiquetas a los recursos de CSPM de Security Hub

Una etiqueta es una etiqueta que puede definir y asignar a AWS los recursos, incluidos ciertos tipos de recursos de AWS Security Hub Cloud Security Posture Management (CSPM). Con las etiquetas, puede identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Por ejemplo, puede usar etiquetas para aplicar políticas, asignar costos, distinguir entre las versiones de los recursos o identificar los recursos que respaldan determinados requisitos de conformidad o flujos de trabajo.

Puede añadir etiquetas a los siguientes tipos de recursos CSPM de Security Hub:

- Reglas de automatización
- Políticas de configuración
- Recurso de Hub

Un recurso puede tener hasta 50 etiquetas. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Una clave de etiqueta es una etiqueta general que actúa como una categoría para un valor de etiqueta más específico. Un valor de etiqueta actúa como descriptor de una clave de etiqueta. Para obtener más información acerca de las opciones y los requisitos de etiquetado, consulte [Conceptos básicos del etiquetado](#).

Para añadir etiquetas a un recurso CSPM de Security Hub, puede utilizar la consola CSPM de Security Hub o la API CSPM de Security Hub. Sin embargo, la consola no permite agregar etiquetas al recurso de Hub.

Después de agregar las etiquetas, puede editarlas y cambiar la clave o el valor.

[Para añadir o editar etiquetas para varios recursos CSPM de Security Hub al mismo tiempo, utilice las operaciones de etiquetado de la API de etiquetado.AWS Resource Groups](#)

Important

La adición de etiquetas a un recurso puede afectar al acceso al recurso. Antes de añadir una etiqueta a un recurso, revise las políticas AWS Identity and Access Management (de IAM) que puedan utilizar etiquetas para controlar el acceso a los recursos.

Console

Para añadir etiquetas a un recurso CSPM de Security Hub (consola)

Al crear una regla de automatización o una política de configuración, la consola CSPM de Security Hub ofrece opciones para añadirle etiquetas. Puede proporcionar la clave y el valor de la etiqueta en la sección Etiquetas.

Security Hub CSPM API

Para añadir etiquetas a un recurso CSPM (API) de Security Hub

Para crear un recurso y añadirle una o más etiquetas mediante programación, utilice la operación adecuada para el tipo de recurso que desee crear:

- Para crear una política de configuración y añadirle una o más etiquetas, invoque la [CreateConfigurationPolicy](#) API o, si la utiliza AWS CLI, ejecute el comando. [create-configuration-policy](#)
- Para crear una regla de automatización y añadirle una o más etiquetas, invoca la [CreateAutomationRule](#) API o, si la utilizas AWS CLI, ejecuta el [create-automation-rule](#) comando.
- Para habilitar el CSPM de Security Hub y añadir una o más etiquetas a su Hub recurso, invoque la [EnableSecurityHub](#) API o, si utiliza AWS Command Line Interface (AWS CLI), ejecute el comando. [enable-security-hub](#)

En su solicitud, use el parámetro `tags` para especificar la clave de etiqueta y el valor de etiqueta opcional de cada etiqueta que quiera añadir al recurso. El parámetro `tags` especifica una matriz de uno o varios objetos. Cada objeto especifica una clave de etiqueta y su valor de etiqueta asociado.

Para añadir una o más etiquetas a un recurso existente, utilice la [TagResource](#) operación de la API CSPM de Security Hub o, si la utiliza AWS CLI, ejecute el comando [tag-resource](#). En su solicitud, especifique el nombre de recurso de Amazon (ARN) del recurso al que desea añadir una etiqueta. Use el parámetro `tags` para especificar la clave de etiqueta (`key`) y el valor de etiqueta opcional (`value`) de cada etiqueta que quiera añadir. El parámetro `tags` especifica una matriz de objetos, un objeto para cada clave de etiqueta y su valor de etiqueta asociado.

Por ejemplo, el siguiente AWS CLI comando agrega una clave de `Environment` etiqueta con un valor de `Prod` etiqueta a la política de configuración especificada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (`\`) de continuación de línea para mejorar la legibilidad.

Ejemplo de comando de la CLI:

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags '{"Environment":"Prod"}'
```

Donde:

- `resource-arn` especifica el ARN de la política de configuración a la que se va a agregar una etiqueta.
- `Environment` es la clave de etiqueta de la etiqueta que se va a añadir a la regla.
- `Prod` es el valor de etiqueta para la clave de etiqueta especificada (`Environment`).

En el siguiente ejemplo, el comando agrega varias etiquetas a la política de configuración.

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags '{"Environment":"Prod", "CostCenter":"12345", "Owner":"jane-doe"}'
```

Para cada objeto de una matriz `tags`, se requieren los argumentos `key` y `value`. Sin embargo, el valor del argumento `value` puede ser una cadena vacía. Si no desea asociar un valor de etiqueta a una clave de etiqueta, no especifique un valor para el argumento `value`. Por ejemplo, el comando siguiente añade una clave de etiqueta `Owner` sin un valor de etiqueta asociado:

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags '{"Owner":""}'
```

Si la operación de etiquetado se realiza correctamente, Security Hub CSPM devuelve una respuesta HTTP 200 vacía. De lo contrario, el CSPM de Security Hub devuelve una respuesta HTTP 4 xx ó 500 que indica el motivo del error de la operación.

Edición de etiquetas para los recursos CSPM de Security Hub

A medida que su entorno o sus requisitos cambien con el tiempo, puede evaluar las etiquetas existentes para los recursos de AWS Security Hub Cloud Security Posture Management (CSPM) y cambiarlas según sea necesario. Puede definir etiquetas y asignarlas a uno o más recursos de AWS, incluidos ciertos tipos de recursos de Macie. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Una clave de etiqueta es una etiqueta general que actúa como una categoría para un valor de etiqueta más específico. Un valor de etiqueta actúa como descriptor de una clave de etiqueta.

Las etiquetas pueden ayudarle a identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Por ejemplo, puede usar etiquetas para aplicar políticas, asignar costos, distinguir entre las versiones de los recursos o identificar los recursos que respaldan determinados requisitos de conformidad o flujos de trabajo.

Puede añadir etiquetas a los siguientes tipos de recursos CSPM de Security Hub:

- Reglas de automatización
- Políticas de configuración
- Recurso de Hub

Para editar las claves o los valores de las etiquetas de un recurso CSPM de Security Hub, puede utilizar la API CSPM de Security Hub. La consola CSPM de Security Hub actualmente no admite la edición de etiquetas.

Important

Modificar las etiquetas de un recurso puede afectar el acceso a él. Antes de editar la etiqueta de un recurso, revise las políticas AWS Identity and Access Management (de IAM) que puedan usar etiquetas para controlar el acceso a los recursos.

Security Hub CSPM API

Para editar las etiquetas de un recurso CSPM (API) de Security Hub

Al editar una etiqueta de un recurso mediante programación, sobrescribe la etiqueta existente con valores nuevos. Por lo tanto, la mejor forma de editar una etiqueta depende de si desea editar

una clave de etiqueta, un valor de etiqueta o ambos. Para editar una clave de etiqueta, [elimine la etiqueta actual](#) y [añada una nueva](#).

Para editar o eliminar solo el valor de etiqueta asociado a una clave de etiqueta, sobrescriba el valor existente mediante la [TagResource](#) operación de la API CSPM de Security Hub. Si utiliza la AWS CLI, ejecute el comando [tag-resource](#). En su solicitud, especifique el nombre de recurso de Amazon (ARN) del recurso cuyo valor de etiqueta desea editar o eliminar.

Para editar el valor de una etiqueta, utilice el parámetro `tags` para especificar la clave de etiqueta cuyo valor de etiqueta desea cambiar. También debe especificar el nuevo valor de etiqueta para la clave. Por ejemplo, el siguiente AWS CLI comando cambia el valor de la etiqueta de `Prod` a `Test` para la clave de `Environment` etiqueta asignada a la regla de automatización especificada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (`\`) de continuación de línea para mejorar la legibilidad.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Test"}'
```

Donde:

- `resource-arn` especifica el ARN de la política de configuración.
- **`Environment`** es la clave de etiqueta asociada al valor de etiqueta que se va a cambiar.
- **`Test`** es el nuevo valor de la etiqueta para la clave especificada (**`Environment`**).

Para eliminar un valor de etiqueta de una clave de etiqueta, no especifique un valor para el argumento `value` de la clave en el parámetro `tags`. Por ejemplo:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

Si la operación se realiza correctamente, Security Hub CSPM devuelve una respuesta HTTP 200 vacía. De lo contrario, el CSPM de Security Hub devuelve una respuesta HTTP 4 xx ó 500 que indica el motivo del error de la operación.

Revisión de etiquetas para los recursos de CSPM de Security Hub

Después de añadir o editar etiquetas para los recursos de AWS Security Hub Cloud Security Posture Management (CSPM), puede ver qué claves y valores de etiqueta tiene actualmente un recurso.

Puede definir etiquetas y asignarlas a uno o más recursos de AWS, incluidos ciertos tipos de recursos de Macie. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Una clave de etiqueta es una etiqueta general que actúa como una categoría para un valor de etiqueta más específico. Un valor de etiqueta actúa como descriptor de una clave de etiqueta.

Las etiquetas pueden ayudarle a identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Por ejemplo, puede usar etiquetas para aplicar políticas, asignar costos, distinguir entre las versiones de los recursos o identificar los recursos que respaldan determinados requisitos de conformidad o flujos de trabajo.

Puede añadir etiquetas a los siguientes tipos de recursos CSPM de Security Hub:

- Reglas de automatización
- Políticas de configuración
- Recurso de Hub

Puede revisar las etiquetas de una regla de automatización o política de configuración de CSPM de Security Hub mediante la consola de CSPM de Security Hub o la API de CSPM de Security Hub. La consola no admite la revisión de las etiquetas del recurso de Hub. Mediante programación, puede revisar las etiquetas de cualquier recurso.

[Para revisar las etiquetas de varios recursos CSPM de Security Hub al mismo tiempo, utilice las operaciones de etiquetado de la API de etiquetado.AWS Resource Groups](#)

Console

Para revisar las etiquetas de un recurso CSPM de Security Hub (consola)

1. Con las credenciales del administrador CSPM de Security Hub, abra la consola de AWS Security Hub Cloud Security Posture Management (CSPM) en. <https://console.aws.amazon.com/securityhub/>
2. Elija una de las siguientes opciones, en función del tipo de recurso al que desea añadir una etiqueta:

- Para revisar las etiquetas de una regla de automatización, seleccione Automatizaciones en el panel de navegación. A continuación, seleccione una regla de automatización.
- Para revisar las etiquetas de una política de configuración, seleccione Configuración en el panel de navegación. A continuación, en la pestaña Políticas, seleccione la opción situada junto a una política de configuración. Se abrirá un panel lateral que mostrará el número de etiquetas asignadas a la política. Puede expandir el encabezado Etiquetas para ver las claves y los valores de las etiquetas.

La sección Etiquetas muestra una lista de todas las etiquetas asignadas actualmente al recurso.

Security Hub CSPM API

Para revisar las etiquetas de un recurso CSPM (API) de Security Hub

Para recuperar y revisar las etiquetas de un recurso existente, invoque la API.

[ListTagsForResource](#) En su solicitud, utilice el parámetro `resourceArn` para especificar el nombre de recurso de Amazon (ARN) del recurso.

Si utiliza el AWS CLI, ejecute el [list-tags-for-resource](#) comando y utilice el `resource-arn` parámetro para especificar el ARN del recurso. Por ejemplo:

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Si la operación se realiza correctamente, Security Hub CSPM devuelve una matriz. `tags` Cada objeto de la matriz especifica una etiqueta (tanto la clave como el valor de la etiqueta) que está asignada actualmente al recurso. Por ejemplo:

```
{
  "tags": [
    {
      "key": "Environment",
      "value": "Prod"
    },
    {
      "key": "CostCenter",
      "value": "12345"
    },
    {
      "key": "Owner",
```

```
        "value": ""
      }
    ]
  }
```

Donde `Environment`, `CostCenter` y `Owner` son las claves de etiqueta que se asignan al recurso. `Prod` es el valor de etiqueta asociado a la clave de etiqueta `Environment`. `12345` es el valor de etiqueta asociado a la clave de etiqueta `CostCenter`. La clave de etiqueta `Owner` no tiene un valor de etiqueta asociado.

Para recuperar una lista de todos los recursos CSPM de Security Hub que tienen etiquetas y todas las etiquetas asignadas a cada uno de esos recursos, utilice la [GetResources](#) operación de la API de AWS Resource Groups etiquetado. En su solicitud, defina el valor del parámetro `ResourceTypeFilters` como `securityhub`. Para ello AWS CLI, ejecute el comando [get-resources](#) y defina el valor del parámetro en. `resource-type-filters securityhub` Por ejemplo:

```
$ aws resourcegroupstaggingapi get-resources --resource-type-filters "securityhub"
```

Si la operación se lleva a cabo correctamente, Resource Groups devuelve una matriz `ResourceTagMappingList`. La matriz contiene un objeto para cada recurso CSPM de Security Hub que tenga etiquetas. Cada objeto especifica el ARN de un recurso CSPM de Security Hub y las claves y valores de etiqueta que se asignan al recurso.

Eliminar etiquetas de los recursos de CSPM de Security Hub

Si añade etiquetas a un recurso de AWS Security Hub Cloud Security Posture Management (CSPM), puede eliminar posteriormente una o más de ellas. Una etiqueta es una etiqueta que se define y se asigna a AWS los recursos, incluidos determinados tipos de recursos CSPM de Security Hub. Puede añadir, editar y eliminar etiquetas de los siguientes tipos de recursos CSPM de Security Hub: reglas de automatización, políticas de configuración y el Hub recurso.

Para eliminar etiquetas de un recurso individual de AWS Security Hub Cloud Security Posture Management (CSPM), puede utilizar la API CSPM de Security Hub. La consola CSPM de Security Hub actualmente no admite la eliminación de etiquetas.

[Para eliminar etiquetas de varios recursos CSPM de Security Hub al mismo tiempo, utilice las operaciones de etiquetado de la API de etiquetado.AWS Resource Groups](#)

⚠ Important

La eliminación de etiquetas de un recurso puede afectar al acceso al recurso. Antes de eliminar una etiqueta, revise las políticas AWS Identity and Access Management (de IAM) que puedan utilizarla para controlar el acceso a los recursos.

Security Hub CSPM API

Para eliminar etiquetas de un recurso CSPM (API) de Security Hub

Para eliminar una o más etiquetas de un recurso mediante programación, utilice la [UntagResource](#) operación de la API CSPM de Security Hub. En su solicitud, utilice el parámetro `resourceArn` para especificar el nombre de recurso de Amazon (ARN) del recurso del que quiere eliminar una etiqueta. Utilice el parámetro `tagKeys` para especificar la clave de etiqueta de la etiqueta que se va a eliminar. Para eliminar varias etiquetas, añada el parámetro `tagKeys` y el argumento de cada etiqueta que desee eliminar, separados por un signo `&`, por ejemplo, `tagKeys=key1&tagKeys=key2`. Para quitar solo un valor de etiqueta específico (no una clave de etiqueta) de un recurso, [edite la etiqueta](#) en lugar de eliminarla.

Si utiliza el comando `untag-resource` AWS CLI, ejecute el comando [untag-resource](#) para eliminar una o más etiquetas de un recurso. Para el parámetro `resource-arn`, especifique el ARN del recurso del que se va a eliminar una etiqueta. Utilice el parámetro `tag-keys` para especificar la clave de etiqueta de la etiqueta que se va a eliminar. Por ejemplo, el siguiente comando elimina la etiqueta `Environment` (tanto la clave como el valor de la etiqueta) de la política de configuración especificada:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

Donde `resource-arn` especifica el ARN de la política de configuración de la que se va a eliminar una etiqueta y `Environment` es la clave de etiqueta de la etiqueta que se va a eliminar.

Para eliminar varias etiquetas de un recurso, agregue cada clave adicional como argumento para el parámetro `tag-keys`: Por ejemplo:

```
$ aws securityhub untag-resource \
```

```
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tag-keys Environment Owner
```

Si la operación se realiza correctamente, Security Hub CSPM devuelve una respuesta HTTP 200 vacía. De lo contrario, el CSPM de Security Hub devuelve una respuesta HTTP 4 xx ó 500 que indica el motivo del error de la operación.

Cuotas para Security Hub CSPM

Cuenta de AWS Tiene determinadas cuotas predeterminadas, anteriormente denominadas límites, para cada una de ellas. Servicio de AWS Estas cuotas establecen el número máximo de recursos u operaciones de servicio que puede haber en su cuenta. En este tema se incluye un enlace a las cuotas que se aplican a los recursos y las operaciones de AWS Security Hub Cloud Security Posture Management (CSPM) de su cuenta. A menos que se indique lo contrario, cada cuota se aplica a su cuenta en cada Región de AWS.

Algunas cuotas pueden aumentarse, mientras que otras no. Para solicitar el aumento de una cuota, use la [consola de Service Quotas](#). Para saber cómo solicitar el aumento de una cuota, consulte [Solicitud de aumento de cuota](#) en la Guía del usuario de Service Quotas. Si no hay una cuota disponible en la consola de Service Quotas, utilice el [formulario de aumento del límite de servicio](#) de la AWS Support Center Console para solicitar un aumento de la cuota.

Cuotas máximas

Para obtener una lista de las cuotas que se aplican a los recursos de CSPM de Security Hub, consulte los [puntos finales y las cuotas de AWS Security Hub Cloud Security Posture Management \(CSPM\)](#) en el. Referencia general de AWS

Cuotas de tarifas

Para obtener una lista de las cuotas que se aplican a las operaciones de la API CSPM de Security Hub, consulte la referencia de la AWS API de [gestión de la postura de seguridad \(CSPM\) de Security Hub Cloud](#).

Si configura la [agregación entre regiones en Security Hub CSPM](#), una llamada a las regiones vinculadas BatchImportFindings y a la región de BatchUpdateFindings agregación afectará a las regiones vinculadas. La operación GetFindings recupera resultados de las regiones vinculadas y la región de agregación. Sin embargo, las operaciones de BatchEnableStandards y UpdateStandardsControl son específicas de cada región.

Historial de documentos de la Guía del usuario de AWS Security Hub

En la siguiente tabla se describen los cambios importantes en la documentación desde la última versión de AWS Security Hub y Security Hub CSPM. En el caso de las versiones de los nuevos controles de seguridad del CSPM, la fecha especifica cuándo empiezan a estar disponibles los controles si son compatibles. Regiones de AWS Los controles pueden tardar entre 1 y 2 semanas en estar disponibles en todas las regiones compatibles.

Para recibir notificaciones sobre las actualizaciones de la Guía del usuario de AWS Security Hub, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Actualizaciones para encontrar la retención	Security Hub CSPM ahora almacena los hallazgos archivados durante 30 días en lugar de 90 días, lo que puede reducir el ruido de las búsquedas. Para una retención a más largo plazo, puedes exportar los resultados a un bucket de S3 mediante una acción personalizada con una regla de Amazon EventBridge .	20 de junio de 2025
Actualización de la política administrada existente	Security Hub CSPM agregó un nuevo permiso a. <code>AWSSecurityHubOrganizationsAccess</code> . El permiso permite a la administración de la organización habilitar y administrar Security Hub y Security Hub CSPM dentro de una organización.	17 de junio de 2025

[Actualización de la política administrada existente](#)

Security Hub CSPM agregó un nuevo permiso a. `AWSSecurityHubFullAccess`. El permiso permite a los directores crear un rol vinculado a un servicio para Security Hub.

[Versión preliminar pública de AWS Security Hub](#)

Publicada una versión preliminar pública de la [Guía del usuario de AWS Security Hub](#).

[Nueva política gestionada para Security Hub](#)

Una nueva política gestionada permite a Security Hub gestionar AWS Config las reglas y los recursos del Security Hub en la organización de un cliente y en su nombre. `AWSSecurityHubV2ServiceRolePolicy`. Security Hub se encuentra en versión preliminar y está sujeto a cambios.

[Actualizaciones de los estándares y controles de seguridad](#)

Eliminamos el [control IAM.10](#) del estándar [PCI](#) DSS v4.0.1. Este control comprueba si las políticas de contraseñas de las cuentas de los usuarios de IAM cumplen los requisitos mínimos, incluida una longitud mínima de contraseña de 7 caracteres. La versión 4.0.1 de PCI DSS ahora requiere que las contraseñas tengan un mínimo de 8 caracteres. El control IAM.10 sigue aplicándose al estándar PCI DSS v3.2.1, que tiene diferentes requisitos de contraseña.

30 de mayo de 2025

[Nuevo estándar de seguridad](#)

Security Hub CSPM ahora proporciona un [estándar de seguridad](#) que se alinea con el marco de ciberseguridad y cumplimiento NIST SP 800-171, revisión 2. Este nuevo estándar incluye más de 60 controles de seguridad existentes. Los controles realizan comprobaciones automatizadas que evalúan el cumplimiento de ciertos requisitos Servicios de AWS y recursos con respecto a un subconjunto de los requisitos definidos en el marco.

29 de mayo de 2025

[Actualizaciones de los controles de seguridad](#)

Security Hub CSPM anuló en total la versión del siguiente control Regiones de AWS: [RDS.46] Las instancias de base de datos de RDS no deberían implementarse en subredes públicas con rutas a puertas de enlace de Internet. Anteriormente, este control era compatible con el estándar AWS Foundational Security Best Practices (FSBP).

8 de mayo de 2025

[Nuevos controles de seguridad](#)

Security Hub CSPM lanzó 9 controles nuevos. La mayoría de los controles son compatibles con el estándar de [mejores prácticas de seguridad AWS fundamentales \(FSBP\)](#).

Algunos de los controles cumplen con los requisitos del [NIST SP 800-53 Rev. 5](#).

7 de mayo de 2025

- [Para el estándar AWS FSBP, IDs los controles aplicables son: DocumentDB.6, RDS.44, RedshiftServerless.2, RedshiftServerless.3, .5, .6 y .7.](#)
- [Para el NIST SP 800-53 Rev. 5, los controles aplicables son: .10, IDs .4 y .7. CloudTrail RedshiftServerless RedshiftServerless](#)

Nuevos controles de seguridad

Security Hub CSPM lanzó 24 controles nuevos. [La mayoría de los controles son compatibles con las mejores prácticas de seguridad AWS fundamentales \(FSBP\) o el estándar de etiquetado de recursos.](#) [AWS](#) Algunos de los controles cumplen con los requisitos del [NIST SP 800-53 Rev. 5](#).

16 de abril de 2025

- [Para el estándar AWS FSBP, IDs los controles aplicables son: EC2.173, RDS.41, RDS.42 y .8.](#)
[SageMaker](#)
- [Para el estándar de etiquetado de AWS recursos, IDs los controles aplicables son: Amplify.1, Amplify.2, Batch.4, DataSync.2, EC2 .174, EC2 .175, EC2 .176, EC2 .177, EC2 .178, .179, Redshift.17, .6, .7, SSM.5, Transfer.4, Transfer.5, EC2 SageMaker SageMaker Transferencia.6 y Transfer.7.](#)
- [Para el NIST SP 800-53 Rev. 5, los controles aplicables son: ECS.17 y IDs RDS.42.](#)

Nuevos controles de seguridad

Security Hub CSPM lanzó cuatro nuevos controles para el estándar [AWS Foundational Security Best Practices](#). Los controles son:

18 de marzo de 2025

- [the section called “\[FSx.3\] FSx para los sistemas de archivos OpenZFS, debe configurarse para el despliegue en zonas de disponibilidad múltiples”](#)
- [the section called “\[FSx.4\] FSx para los sistemas de archivos NetApp ONTAP, debe configurarse para el despliegue en zonas de disponibilidad múltiples”](#)
- [the section called “\[FSx.5\] FSx para Windows, los sistemas de archivos del servidor de archivos deben configurarse para el despliegue en zonas de disponibilidad múltiples”](#)
- [the section called “Los grupos de trabajo de Amazon Redshift Serverless deben utilizar un enrutamiento de RedshiftServerless VPC mejorado”](#)

[Actualizaciones de los estándares y controles de seguridad](#)

Eliminamos el [control de seguridad RDS.18](#) del estándar AWS básico de mejores prácticas de seguridad y automatizamos las comprobaciones para cumplir con los requisitos del NIST SP 800-53 Rev. 5. Desde que se retiraron las redes Amazon EC2 -Classic, las instancias de Amazon Relational Database Service (Amazon RDS) ya no se pueden implementar fuera de una VPC. [El control sigue formando parte del estándar de administración de servicios .AWS Control Tower](#)

7 de marzo de 2025

[Actualizaciones de los hallazgos de control](#)

El CSPM de Security Hub ahora genera WARNING resultados para un control habilitado si el [registro de recursos](#) no está activado AWS Config para el tipo de recurso que el control comprueba. Esto puede ayudarlo a identificar y abordar posibles brechas de configuración en sus comprobaciones de control de seguridad.

25 de febrero de 2025

Nuevos controles de seguridad

Security Hub CSPM lanzó 11 controles nuevos. Los controles son:

24 de febrero de 2025

- the section called “[Connect .2] Las instancias de Amazon Connect deben tener el CloudWatch registro activado”
- the section called “[ECR.5] Los repositorios de ECR deben estar cifrados y gestionados por el cliente AWS KMS keys”
- the section called “[ELB.17] Los balanceadores de carga de redes y aplicaciones que utilizan dispositivos de escucha deben usar las políticas de seguridad recomendadas”
- the section called “[Glue.4] Los trabajos de AWS Glue Spark deberían ejecutarse en versiones compatibles de AWS Glue”
- the section called “[GuardDuty.11] La monitorización del GuardDuty tiempo de ejecución debe estar habilitada”
- the section called “[GuardDuty.12] La monitorización del tiempo de ejecución de

GuardDuty ECS debe estar habilitada”

- the section called “[GuardDuty.13] La monitorización del GuardDuty EC2 tiempo de ejecución debe estar habilitada”
- the section called “Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de cambio de subred”
- the section called “[RDS.40] Las instancias de base de datos de RDS para SQL Server deberían publicar los registros en Logs CloudWatch ”
- the section called “[SQS.3] Las políticas de acceso a las colas de SQS no deberían permitir el acceso público”
- the section called “[Transfer.3] Los conectores Transfer Family deben tener habilitado el registro”

Nuevos controles de seguridad

Security Hub CSPM lanzó 37 controles nuevos para el estándar de [etiquetado AWS de recursos](#). Security Hub CSPM también lanzó los siguientes controles nuevos:

22 de enero de 2025

- [the section called “\[EMR.3\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en reposo”](#)
- [the section called “\[EMR.4\] Las configuraciones de seguridad de Amazon EMR deben cifrarse en tránsito”](#)
- [the section called “\[SageMaker.5\] SageMaker los modelos deberían bloquear el tráfico entrante”](#)

Nuevo control de seguridad

Security Hub CSPM publicó [EC2.172 La configuración de acceso público del bloque de EC2 VPC debería bloquear el tráfico de las puertas de enlace de Internet](#).

15 de enero de 2025

Nuevos controles de seguridad

Están disponibles los siguientes controles CSPM nuevos de Security Hub. 17 de diciembre de 2024

- the section called “[Cognito.1] Los grupos de usuarios de Cognito deberían tener activada la protección contra amenazas con un modo de aplicación de funciones completas para la autenticación estándar”
- the section called “[RDS.38] Las instancias de base de datos de RDS para PostgreSQL deben cifrarse en tránsito”
- the section called “[RDS.39] Las instancias de base de datos de RDS para MySQL deben cifrarse en tránsito”
- the section called “[Redshift.16] Los grupos de subredes de clústeres de Redshift deben tener subredes de varias zonas de disponibilidad”

[Security Hub CSPM es compatible con PCI DSS v4.0.1](#)

Security Hub CSPM ahora es compatible con la versión 4.0.1 del Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS). Para obtener más información sobre el estándar y los controles que se le aplican, consulte [PCI DSS en Security Hub](#) CSPM.

11 de diciembre de 2024

[Security Hub \(CSPM\) recibe los resultados de la secuencia de GuardDuty ataque](#)

Security Hub CSPM ahora recibe los resultados de la secuencia de ataques de Amazon GuardDuty Extended Threat Detection. Los detalles de búsqueda de la secuencia de ataque están disponibles en el objeto de [detección](#) del formato de búsqueda de AWS seguridad (ASFF).

1 de diciembre de 2024

[Security Hub \(CSPM\) compatible con el nuevo Región de AWS](#)

Security Hub CSPM ya está disponible en la región de Asia Pacífico (Malasia). Algunos controles de seguridad tienen limitaciones regionales. Para obtener una lista de los controles que no están disponibles en esta región, consulte [Límites regionales de los controles CSPM de Security Hub](#).

22 de noviembre de 2024

Cambios en la configuración.1

Security Hub CSPM aumentó la severidad del control de la Config.1 de MEDIUM a CRITICAL y agregó nuevos códigos de estado y motivos de estado por los errores en los hallazgos de la Config.1. Para obtener más información sobre los cambios, consulte la entrada del 20 de noviembre de 2024 en el [registro de cambios de los controles CSPM de Security Hub](#).

20 de noviembre de 2024

[Nuevos controles de seguridad](#)

Están disponibles los siguientes controles CSPM nuevos de Security Hub. Estos controles forman parte de las prácticas recomendadas de seguridad AWS fundamentales y del NIST SP 800-53 Rev. 5, y evalúan si una nube privada virtual (VPC) que usted administra tiene un punto final de VPC de interfaz para un recurso o recurso. Servicio de AWS AWS

15 de noviembre de 2024

- [the section called “\[EC2.55\] VPCs debe configurarse con un punto final de interfaz para la API ECR”](#)
- [the section called “\[EC2.56\] VPCs debe configurarse con un punto final de interfaz para Docker Registry”](#)
- [the section called “\[EC2.57\] VPCs debe configurarse con un punto final de interfaz para Systems Manager”](#)
- [the section called “\[EC2.58\] VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager”](#)
- [the section called “\[EC2.60\] VPCs debe configurarse con un punto final de interfaz](#)

[para Systems Manager
Incident Manager”](#)

Nuevos controles de seguridad

Están disponibles los siguientes controles CSPM nuevos de Security Hub. 18 de octubre de 2024

- [the section called “\[AppSync .1\] Las cachés de las AWS AppSync API deben cifrarse en reposo”](#)
- [the section called “\[AppSync .6\] Las cachés de las AWS AppSync API deben cifrarse en tránsito”](#)
- [the section called “\[EC2.170\] Las plantillas de EC2 lanzamiento deben usar el servicio de metadatos de instancias versión 2 \(\) IMDSv2”](#)
- [the section called “\[EC2.171\] Las conexiones EC2 VPN deben tener el registro habilitado”](#)
- [the section called “\[EFS.8\] Los sistemas de archivos de EFS deben cifrarse en reposo”](#)
- [the section called “\[KMS.5\] Las claves KMS no deben ser de acceso público”](#)
- [the section called “\[SNS.4\] Las políticas de acceso a los temas de SNS no deberían permitir el acceso público”](#)

Nuevos controles de seguridad

Están disponibles los siguientes controles CSPM nuevos de Security Hub. 3 de octubre de 2024

- [the section called “\[ECS.16\] Los conjuntos de tareas de ECS no deben asignar automáticamente direcciones IP públicas”](#)
- [the section called “\[GuardDuty.7\] La supervisión en tiempo de ejecución de GuardDuty EKS debe estar habilitada”](#)
- [the section called “\[Kinesis.3\] Las transmisiones de Kinesis deben tener un periodo adecuado de retención de datos”](#)
- [the section called “\[MSK.3\] Los conectores de MSK Connect deben cifrarse en tránsito”](#)
- [the section called “\[RDS.36\] Las instancias de base de datos de RDS para PostgreSQL deben publicar registros en Logs CloudWatch ”](#)
- [the section called “\[RDS.37\] Los clústeres de bases de datos Aurora PostgreSQL deberían publicar registros en Logs CloudWatch ”](#)

- [the section called “\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público”](#)

Nuevos controles de seguridad

Están disponibles los siguientes controles CSPM nuevos de Security Hub. 30 de agosto de 2024

- [the section called “\[Athena.4\] Los grupos de trabajo de Athena deben tener el registro habilitado”](#)
- [the section called “\[CodeBuild.7\] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo”](#)
- [the section called “\[DataSync.1\] DataSync las tareas deberían tener el registro activado”](#)
- [the section called “\[EFS.7\] Los sistemas de archivos de EFS deben tener habilitadas las copias de seguridad automáticas”](#)
- Glue.2 (retirado)
- [the section called “\[Glue.3\] Las transformaciones AWS Glue de aprendizaje automático deben cifrarse en reposo”](#)
- [the section called “\[WorkSpaces.1\] los volúmenes de WorkSpaces usuarios deben cifrarse en reposo”](#)
- [the section called “\[WorkSpaces.2\] los volúmenes](#)

WorkSpaces raíz deben cifrarse en reposo”

Nuevo panel de resultados

El [nuevo panel de búsqueda](#) de la consola CSPM de Security Hub le ayuda a tomar medidas rápidamente en relación con los hallazgos , revisar los detalles de los recursos y el historial de búsquedas, y encontrar otra información pertinente sobre un hallazgo.

16 de agosto de 2024

Actualización del control Config.1

El [control Config.1](#) comprueba si AWS Config está habilitado, utiliza la función vinculada al servicio y registra los recursos de los controles habilitados. Security Hub CSPM agregó un parámetro de control personalizado denominado `includeConfigServiceLinkedRoleCheck` . Si establece este parámetro en `false`, puede optar por no comprobar si AWS Config utiliza el rol vinculado al servicio.

15 de agosto de 2024

[Designación de una región de origen sin regiones vinculadas](#)

Ahora puede crear un agregador de búsquedas y establecer una región de origen sin vincular ninguna Regiones de AWS a la región de origen. Esto permite habilitar la [configuración centralizada](#) sin especificar las regiones vinculadas.

25 de julio de 2024

[Selección de los controles disponibles en más regiones](#)

15 de julio de 2024

Los siguientes controles ya están disponibles en forma adicional Regiones de AWS, incluidos EE. UU. Este (Norte de Virginia) y EE. UU. Este (Ohio).

- [the section called “\[DataFirehose.1\] Los flujos de entrega de Firehose deben cifrarse en reposo”](#)
- [the section called “\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM”](#)
- [the section called “\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado”](#)
- [the section called “\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado”](#)
- [the section called “\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito”](#)
- [the section called “\[EFS.6\] Los destinos de montaje de EFS no deben estar](#)

- [asociados a una subred pública](#)
- [the section called “\[EKS.3\] Los clústeres de EKS deben usar secretos de Kubernetes cifrados”](#)
- [the section called “\[FSx.2\] FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad”](#)
- [the section called “\[MQ.2\] Los corredores de ActiveMQ deberían transmitir los registros de auditoría a CloudWatch”](#)
- [the section called “\[MQ.3\] Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias”](#)
- [the section called “Los OpenSearch dominios \[Opensearch.11\] deben tener al menos tres nodos principales dedicados”](#)
- [the section called “\[Redshift.15\] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos”](#)
- [the section called “\[SageMaker.4\] Las](#)

variantes de producción de SageMaker terminales deben tener un recuento inicial de instancias superior a 1”

- the section called “[Service Catalog.1] Las carteras de Service Catalog solo deben compartirse dentro de una AWS organización”
- the section called “[Transfer.2] Los servidores de Transfer Family no deben utilizar el protocolo FTP para la conexión del punto de conexión”

Nuevos controles de seguridad

Están disponibles los siguientes controles CSPM nuevos de Security Hub: 11 de julio de 2024

- [the section called “\[GuardDuty.5\] La supervisión de registros de auditoría de GuardDuty EKS debe estar habilitada”](#)
- [the section called “\[GuardDuty.6\] La protección de GuardDuty Lambda debe estar habilitada”](#)
- [the section called “\[GuardDuty.8\] La protección contra GuardDuty malware para EC2 debe estar habilitada”](#)
- [the section called “\[GuardDuty.9\] La protección de GuardDuty RDS debe estar habilitada”](#)
- [the section called “\[GuardDuty.10\] La protección de GuardDuty S3 debe estar habilitada”](#)
- [the section called “\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado”](#)
- [the section called “\[Inspector.2\] El análisis de ECR en Amazon Inspector debe estar habilitado”](#)
- [the section called “\[Inspector.3\] El análisis de código](#)

[de Lambda en Amazon Inspector debe estar habilitado”](#)

- [the section called “\[Inspect or.4\] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado”](#)

[Publicación de CIS AWS
Foundations Benchmark
v3.0.0](#)

Security Hub CSPM publicó [Center for Internet Security \(CIS\) AWS Foundations Benchmark v3.0.0](#). La versión incluye los siguientes controles nuevos, así como asignaciones a varios controles existentes.

13 de mayo de 2024

- [the section called “\[EC2.53\] Los grupos EC2 de seguridad no deberían permitir la entrada de 0.0.0.0/0 a los puertos de administración de servidores remotos”](#)
- [the section called “\[EC2.54\] Los grupos EC2 de seguridad no deberían permitir la entrada de :/0 a los puertos de administración de servidores remotos”](#)
- [the section called “\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse”](#)
- [the section called “\[IAM.27\] Las identidades de IAM no deben tener adjunta la política AWSCloud ShellFull Access ”](#)
- [the section called “\[IAM.28\] El analizador de acceso externo del Analizador](#)

de acceso de IAM debe habilitarse”

- the section called “[S3.22] Los buckets de uso general de S3 deben registrar eventos de escritura a nivel de objeto”
- the section called “[S3.23] Los buckets de uso general de S3 deben registrar eventos de lectura a nivel de objeto”

Nuevos controles de seguridad

Están disponibles los siguientes controles CSPM nuevos de Security Hub: 3 de mayo de 2024

- [the section called “\[DataFirehose.1\] Los flujos de entrega de Firehose deben cifrarse en reposo”](#)
- [the section called “\[DMS.10\] Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM”](#)
- [the section called “\[DMS.11\] Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado”](#)
- [the section called “\[DMS.12\] Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado”](#)
- [the section called “\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito”](#)
- [the section called “\[EFS.6\] Los destinos de montaje de EFS no deben estar asociados a una subred pública”](#)

- [the section called “\[EKS.3\] Los clústeres de EKS deben usar secretos de Kubernetes cifrados”](#)
- [the section called “\[FSx.2\] FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad”](#)
- [the section called “\[MQ.2\] Los corredores de ActiveMQ deberían transmitir los registros de auditoría a CloudWatch”](#)
- [the section called “\[MQ.3\] Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias”](#)
- [the section called “Los OpenSearch dominios \[Opensearch.11\] deben tener al menos tres nodos principales dedicados”](#)
- [the section called “\[Redshift.15\] Los grupos de seguridad de Redshift deberían permitir la entrada en el puerto del clúster solo desde orígenes restringidos”](#)
- [the section called “\[SageMaker.4\] Las variantes de producción de SageMaker terminale](#)

[s deben tener un recuento inicial de instancias superior a 1”](#)

- [the section called “\[Service Catalog.1\] Las carteras de Service Catalog solo deben compartirse dentro de una AWS organización”](#)
- [the section called “\[Transfer.2\] Los servidores de Transfer Family no deben utilizar el protocolo FTP para la conexión del punto de conexión”](#)

[AWS Estándar de etiquetado de recursos](#)

El [estándar de etiquetado de AWS recursos](#) de Security Hub CSPM ya está disponible de forma general, junto con los nuevos controles que se aplican al estándar.

30 de abril de 2024

[Actualización de la política administrada existente](#)

Security Hub CSPM actualizó la [política AWS gestionada](#) denominada AmazonSecurityHubFullAccess para obtener información detallada sobre los precios de los Servicios de AWS y los productos.

24 de abril de 2024

Configuración en contexto de los parámetros de control	Si utiliza la configuración central, ahora puede configurar los parámetros de control en contexto , desde la página de detalles de un control de la consola CSPM de Security Hub.	29 de marzo de 2024
Actualización de la política administrada existente	Security Hub CSPM actualizó la política AWS administrada nombrada <code>AWSSecurityHubReadOnlyAccess</code> agregando un <code>Sid</code> campo.	22 de febrero de 2024
Nuevo control de seguridad	El control [Macie.2] La detección automática de datos confidenciales de Macie debe estar habilitada ya está disponible. Para conocer los límites regionales de este control, consulte Availability of controls by Region .	19 de febrero de 2024
Security Hub CSPM disponible en el oeste de Canadá (Calgary)	Security Hub CSPM ya está disponible en el oeste de Canadá (Calgary). Todas las funciones CSPM de Security Hub ya están disponibles en esta región, con la excepción de algunos controles de seguridad. Para obtener más información, consulte Disponibilidad de controles por región .	20 de diciembre de 2023

Nuevos controles de seguridad

Están disponibles los siguientes controles CSPM nuevos de Security Hub: 14 de diciembre de 2023

- the section called “[Backup.1] Los puntos AWS Backup de recuperación deben cifrarse en reposo”
- the section called “[DynamoDB.6] Las tablas de DynamoDB deben tener la protección contra eliminación habilitada”
- the section called “[EC251] Los puntos de conexión EC2 Client VPN deben tener habilitado el registro de conexiones de clientes”
- the section called “[EKS.8] Los clústeres de EKS deben tener habilitado el registro de auditoría”
- the section called “[EMR.2] La configuración de bloqueo del acceso público de Amazon EMR debe estar habilitada”
- the section called “[FSx.1] en el caso FSx de OpenZFS, los sistemas de archivos deben configurarse para copiar etiquetas en copias de seguridad y volúmenes”

- [the section called “\[Macie.1\] Amazon Macie debe estar habilitado”](#)
- [the section called “\[MSK.2\] Los clústeres de MSK deberían tener configurada una supervisión mejorada”](#)
- [the section called “\[Neptune .9\] Los clústeres de base de datos de Neptune se deben implementar en varias zonas de disponibilidad”](#)
- [the section called “Los NetworkFirewall firewalls de Network Firewall se deben implementar en varias zonas de disponibilidad”](#)
- [the section called “\[Network Firewall.2\] El registro de Network Firewall debe estar habilitado”](#)
- [the section called “Los OpenSearch dominios \[Opensearch.10\] deben tener instalada la última actualización de software”](#)
- [the section called “La autoridad emisora de certificados AWS Private CA raíz \[PCA.1\] debe estar deshabilitada”](#)
- [the section called “\[S3.19\] Los puntos de acceso de S3 deben tener habilitada la](#)

[configuración de Bloqueo de acceso público”](#)

- [the section called “\[S3.20\] Los buckets de uso general de S3 deben tener habilidad a la eliminación de MFA”](#)

[Enriquecimiento de resultados](#)

Security Hub CSPM agregó los nuevos campos `AwsAccountName` de búsqueda y `ApplicationName` al formato de búsqueda de AWS seguridad (ASFF). `ApplicationArn`

27 de noviembre de 2023

[Mejoras en el panel Resumen](#)

Ahora puede acceder a más widgets de panel en la página de resumen de la consola CSPM de Security Hub, guardar conjuntos de filtros de panel para centrarse rápidamente en problemas de seguridad específicos y personalizar el diseño del panel.

27 de noviembre de 2023

[Configuración centralizada](#)

La configuración centralizada ya está disponible. Con una configuración central, el administrador delegado de CSPM de Security Hub puede configurar el CSPM, los estándares y los controles de Security Hub en varias cuentas, unidades organizativas () OUs y regiones de la organización.

27 de noviembre de 2023

[Actualizaciones a políticas administradas](#)

Security Hub CSPM agregó nuevos permisos a la política `AWSecurityHubServiceRolePolicy` administrada que permiten a Security Hub CSPM leer y actualizar propiedades de control de seguridad personalizables.

26 de noviembre de 2023

[Personalización de los parámetros de control](#)

Ahora puede personalizar los valores de los parámetros para determinados controles CSPM de Security Hub. Esto puede hacer que los resultados de un control específico sean más relevantes para los requisitos de su empresa y sus expectativas de seguridad.

26 de noviembre de 2023

[Actualizaciones de las políticas administradas](#)

Security Hub CSPM actualizó `AWSecurityHubFullAccess` y `AWSecurityHubOrganizationsAccess` gestionó las políticas que le permiten utilizar, respectivamente, las funciones de Security Hub CSPM y la integración con AWS Organizations

16 de noviembre de 2023

Los controles de seguridad existentes se agregaron al estándar gestionado por el servicio: AWS Control Tower

Se han agregado los siguientes controles CSPM de Security Hub existentes a Service-Managed Standard: AWS Control Tower

14 de noviembre de 2023

- ACM.2
- AppSync5.
- CloudTrail6.
- DMS.9
- DocumentDB.3
- Dynamo DB.3
- EC2.23
- EKS.1
- ElastiCache3.
- ElastiCache4.
- ElastiCache5.
- ElastiCache6.
- EventBridge3.
- KMS.4
- Lambda 3
- MQ.5
- MQ.6
- MSK.1
- RDS.12
- RDS.15
- S3.17

[Actualizaciones a la política administrada](#)

Security Hub CSPM agregó un nuevo permiso de etiquetado a la política `AWSSecurityHubServiceRolePolicy` administrada que permite a Security Hub CSPM leer las etiquetas de recursos relacionadas con los hallazgos.

7 de noviembre de 2023

Nuevos controles de seguridad

Están disponibles los siguientes controles CSPM nuevos de Security Hub: 10 de octubre de 2023

- [the section called “\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves de API”](#)
- [the section called “\[DMS.6\] Las instancias de replicación de DMS deben tener habilitada la actualización automática de las versiones secundarias”](#)
- [the section called “\[DMS.7\] Las tareas de replicación de DMS para la base de datos de destino deben tener habilitado el registro”](#)
- [the section called “\[DMS.8\] Las tareas de replicación del DMS para la base de datos de origen deben tener habilitado el registro”](#)
- [the section called “\[DMS.9\] Los puntos finales del DMS deben usar SSL”](#)
- [the section called “\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas”](#)
- [the section called “\[DocumentDb.4\] Los](#)

clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch ”

- the section called “[DocumentDb.5] Los clústeres de Amazon DocumentDB deben tener habilitada la protección contra eliminaciones”
- the section called “[ECS.9] Las definiciones de tareas de ECS deben tener una configuración de registro”
- the section called “[EventBridge.3] Los autobuses de eventos EventBridge personalizados deben incluir una política basada en los recursos”
- the section called “[EventBridge.4] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos”
- the section called “[MSK.1] Los clústeres de MSK deben cifrarse en tránsito entre los nodos intermedios”
- the section called “[MQ.5] Los corredores ActiveMQ deben usar el modo de

implementación activo/en espera”

- the section called “[MQ.6] Los corredores de RabbitMQ deberían usar el modo de implementación de clústeres”
- the section called “Los NetworkFirewall firewalls de Network Firewall deben tener habilitada la protección de eliminación”
- the section called “[RDS.34] Los clústeres de bases de datos Aurora MySQL deberían publicar los registros de auditoría en Logs CloudWatch ”
- the section called “Los clústeres de bases de datos de RDS [RDS.35] deben tener habilitada la actualización automática de las versiones secundarias”
- the section called “Las zonas alojadas públicas de Route 53 [Route53.2] deben registrar las consultas de DNS”
- the section called “AWS WAF Las reglas de [WAF.12] deben tener habilitadas las métricas CloudWatch ”

[Actualizaciones a la política administrada](#)

Security Hub CSPM agregó nuevas acciones de Organizations a la política `AWSSecurityHubServiceRolePolicy` administrada que permiten a Security Hub CSPM recuperar información de cuentas y unidades organizativas (OU). También agregamos nuevas acciones CSPM de Security Hub que permiten a Security Hub CSPM leer y actualizar las configuraciones de los servicios, incluidos los estándares y los controles.

27 de septiembre de 2023

Los controles de seguridad existentes se han añadido al estándar gestionado por el servicio: AWS Control Tower

Se han agregado los siguientes controles CSPM de Security Hub existentes a Service-Managed Standard: AWS Control Tower

26 de septiembre de 2023

- the section called “[Athena.1] Los grupos de trabajo de Athena deben estar cifrados en reposo”
- the section called “[DocumentDB.1] Los clústeres de Amazon DocumentDB deben cifrarse en reposo”
- the section called “[DocumentDb.2] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado”
- the section called “[Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo”
- the section called “[Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch ”
- the section called “[Neptune.3] Las instantáneas del clúster de base de datos

de Neptune no deben ser públicas”

- the section called “[Neptune .4] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación”
- the section called “[Neptune .5] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas”
- the section called “[Neptune .6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo”
- the section called “[Neptune .7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM”
- the section called “[Neptune .8] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas”
- the section called “Los clústeres de bases de datos de RDS [RDS.27] deben cifrarse en reposo”

[La vista de los controles consolidados y los resultados de los controles consolidados están disponibles en AWS GovCloud \(US\)](#)

La vista de los controles consolidados y los resultados de los controles consolidados ya están disponibles en AWS GovCloud (US) Region. La página de controles de la consola CSPM de Security Hub muestra todos los controles según los estándares. Cada control tiene el mismo ID de control para todos los estándares. Al activar los resultados de control consolidados, recibirá un único resultado por control de seguridad, incluso cuando un control se aplique a varios estándares habilitados.

6 de septiembre de 2023

[La vista de los controles consolidados y los resultados de los controles consolidados están disponibles en las regiones de China](#)

La vista de controles consolidados y los resultados de controles consolidados ahora ya están disponibles en las regiones de China. La página de controles de la consola CSPM de Security Hub muestra todos los controles según los estándares. Cada control tiene el mismo ID de control para todos los estándares. Al activar los resultados de control consolidados, recibirá un único resultado por control de seguridad, incluso cuando un control se aplique a varios estándares habilitados.

[Security Hub CSPM disponible en la región de Israel \(Tel Aviv\)](#)

Security Hub CSPM ya está disponible en Israel (Tel Aviv). Todas las funciones CSPM de Security Hub ya están disponibles en esta región, con la excepción de algunos controles de seguridad. Para obtener más información, consulte [Disponibilidad de controles por región](#).

Nuevos controles de seguridad

Están disponibles los siguientes controles CSPM nuevos de Security Hub: 28 de julio de 2023

- [the section called “\[Athena.1\] Los grupos de trabajo de Athena deben estar cifrados en reposo”](#)
- [the section called “\[DocumentDB.1\] Los clústeres de Amazon DocumentDB deben cifrarse en reposo”](#)
- [the section called “\[DocumentDb.2\] Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado”](#)
- [the section called “\[Neptune.1\] Los clústeres de bases de datos de Neptune deben cifrarse en reposo”](#)
- [the section called “\[Neptune.2\] Los clústeres de bases de datos de Neptune deberían publicar los registros de auditoría en Logs CloudWatch ”](#)
- [the section called “\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas”](#)

- [the section called “\[Neptune .4\] Los clústeres de base de datos de Neptune deben tener habilitada la protección de eliminación”](#)
- [the section called “\[Neptune .5\] Los clústeres de bases de datos de Neptune deberían tener habilitadas las copias de seguridad automáticas”](#)
- [the section called “\[Neptune .6\] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo”](#)
- [the section called “\[Neptune .7\] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM”](#)
- [the section called “\[Neptune .8\] Los clústeres de base de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas”](#)
- [the section called “Los clústeres de bases de datos de RDS \[RDS.27\] deben cifrarse en reposo”](#)

[Nuevos operadores para los criterios de las reglas de automatización](#)

Ahora puede utilizar los operadores de comparación CONTAINS y NOT_CONTAINS para el mapa de reglas de automatización y los criterios de cadena.

25 de julio de 2023

[Reglas de automatización](#)

Security Hub CSPM ahora ofrece reglas de automatización que actualizan automáticamente los hallazgos en función de los criterios que especifique.

13 de junio de 2023

[Nueva integración de terceros](#)

Snykes una nueva integración de terceros que envía los resultados al Security Hub CSPM.

12 de junio de 2023

Los controles de seguridad existentes se han agregado al estándar gestionado por el servicio: AWS Control Tower

Se han agregado los siguientes controles CSPM de Security Hub existentes a Service-Managed Standard: AWS Control Tower

12 de junio de 2023

- the section called “[Cuenta.1] La información de contacto de seguridad debe proporcionarse para un Cuenta de AWS”
- the section called “[APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización”
- the section called “[APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway”
- the section called “[CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados”
- the section called “[EC2.25] Las plantillas de EC2 lanzamiento de Amazon no deben asignar interfaces públicas IPs a las de red”
- the section called “[ELB.1] El equilibrador de carga de aplicación debe configurarse para redirigir todas las solicitudes HTTP a HTTPS”
- the section called “Los clústeres de Redshift

[Redshift.10] deben cifrarse en reposo”

- the section called “[SageMaker.2] las instancias de SageMaker notebook deben lanzarse en una VPC personalizada”
- the section called “[SageMaker.3] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook”
- the section called “La AWS WAF web de [WAF.10] ACLs debe tener al menos una regla o grupo de reglas”

Nuevos controles de seguridad

Están disponibles los siguientes controles CSPM nuevos de Security Hub: 6 de junio de 2023

- the section called “[ACM.2] Los certificados RSA administrados por ACM deben utilizar una longitud de clave de al menos 2048 bits”
- the section called “[AppSync.2] AWS AppSync debe tener habilitado el registro a nivel de campo”
- the section called “[CloudFront.13] CloudFront Las distribuciones deben usar el control de acceso de origen”
- the section called “[Elastic Beanstalk.3] Elastic Beanstalk debería transmitir los registros a CloudWatch”
- the section called “[S3.17] Los depósitos de uso general de S3 deben cifrarse en reposo con AWS KMS keys”
- the section called “[StepFunctions.1] Las máquinas de estado de Step Functions deberían tener el registro activado”

[Security Hub CSPM disponible en Asia Pacífico \(Melbourne\)](#)

Security Hub CSPM ya está disponible en Asia Pacífico (Melbourne). Todas las funciones CSPM de Security Hub ya están disponibles en esta región, con la excepción de algunos controles de seguridad. Para obtener más información, consulte [Disponibilidad de controles por región](#).

25 de mayo de 2023

[Búsqueda del historial](#)

Security Hub CSPM ahora puede rastrear el historial de un hallazgo durante los últimos 90 días.

4 de mayo de 2023

[Nuevos controles de seguridad](#)

Están disponibles los siguientes controles CSPM nuevos de Security Hub: 29 de marzo de 2023

- [the section called “\[EKS.1\] Los puntos de enlace del clúster EKS no deben ser de acceso público”](#)
- [the section called “\[ELB.16\] Los equilibradores de carga de aplicaciones deben estar asociados a una ACL web de AWS WAF”](#)
- [the section called “Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo”](#)
- [the section called “\[S3.15\] Los buckets de uso general de S3 deben tener habilitado el bloqueo de objetos”](#)

[Soporte ampliado para los resultados de control consolidados](#)

La [respuesta de seguridad automatizada de la AWS versión 2.0.0](#) ahora admite los hallazgos de control consolidados. 24 de marzo de 2023

[Security Hub CSPM disponible en versión nueva Regiones de AWS](#)

Security Hub CSPM ya está disponible en Asia Pacífico (Hyderabad), Europa (España) y Europa (Zúrich). Existen límites en cuanto a los controles disponibles en estas regiones. 21 de marzo de 2023

[Actualización a la política administrada](#)

Security Hub CSPM ha actualizado un permiso existente en la política `AWSecurityHubServiceRolePolicy` gestionada.

17 de marzo de 2023

[Nuevos controles de seguridad para el estándar NIST 800-53](#)

3 de marzo de 2023

Security Hub CSPM ha agregado los siguientes controles de seguridad, que son aplicables al estándar NIST 800-53:

- [the section called “\[Account .2\] Cuentas de AWS debe formar parte de una organización AWS Organizations”](#)
 - [the section called “\[CloudWatch.15\] CloudWatch las alarmas deben tener configuradas acciones específicas”](#)
 - [the section called “\[CloudWatch.16\] Los grupos de CloudWatch registros deben retenerse durante un periodo específico”](#)
 - [the section called “\[CloudWatch.17\] las acciones CloudWatch de alarma deben estar activadas”](#)
 - [the section called “\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad”](#)
 - [the section called “\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de copias de seguridad”](#)
-

- EC2.29 — EC2 las instancias deben lanzarse en una VPC (retiradas)
- [the section called “Las instancias de base de datos de RDS \[RDS.26\] deben protegerse mediante un plan de copias de seguridad”](#)
- [the section called “\[S3.14\] Los buckets de uso general de S3 deben tener habilitad o el control de versiones”](#)
- [the section called “El registro de ACL AWS WAF web de \[WAF.11\] debe estar habilitado”](#)

[National Institute of Standards and Technology \(NIST, Instituto Nacional de Estándares y Tecnología\) 800-53, Rev. 5](#)

Security Hub CSPM ahora es compatible con el estándar NIST 800-53 Rev. 5 con más de 200 controles de seguridad aplicables.

28 de febrero de 2023

[Vista de controles consolidados y control de resultados](#)

Con el lanzamiento de la vista de controles consolidados, la página de controles de la consola CSPM de Security Hub muestra todos los controles según los estándares. Cada control tiene el mismo ID de control para todos los estándares. Al activar los resultados de control consolidados, recibirá un único resultado por control de seguridad, incluso cuando un control se aplique a varios estándares habilitados.

23 de febrero de 2023

Nuevos controles de seguridad

Están disponibles los siguientes controles CSPM nuevos de Security Hub. Algunos controles tienen restricciones regionales.

16 de febrero de 2023

- the section called “[ElastiCache.1] Los clústeres ElastiCache (Redis OSS) deben tener habilitadas las copias de seguridad automáticas”
- the section called “[ElastiCache.2] ElastiCache Los clústeres deberían tener habilitadas las actualizaciones automáticas de las versiones secundarias”
- the section called “[ElastiCache.3] los grupos de ElastiCache replicación deberían tener habilitada la conmutación por error automática”
- the section called “[ElastiCache.4] los grupos de ElastiCache replicación deben estar cifrados en reposo”
- the section called “[ElastiCache.5] los grupos de ElastiCache replicación deben cifrarse en tránsito”
- the section called “[ElastiCache.6] Los grupos de

[replicación ElastiCache \(Redis OSS\) de versiones anteriores deberían tener habilitada la autenticación de Redis OSS”](#)

- [the section called “\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado”](#)

[Nuevos campos del ASFF](#)

Se ha agregado Security Hub CSPM. ProductFields ArchivalReasonsSe ha agregado Security Hub ProductFields CSPM. ----SEP----:0/Descripción y. ArchivalReasons:0/Descripción ReasonCode y. AWS ----sep----:0/ al formato de búsqueda de seguridad (ASFF).

8 de febrero de 2023

[Nuevos campos del ASFF](#)

Security Hub CSPM ha añadido el cumplimiento. AssociatedStandards y cumplimiento. SecurityControlId al formato AWS de búsqueda de seguridad (ASFF).

31 de enero de 2023

[Los detalles de la vulnerabilidad ya están disponibles](#)

Ahora puede ver los detalles de la vulnerabilidad en la consola CSPM de Security Hub para ver los hallazgos que Amazon Inspector envía al Security Hub CSPM.

14 de enero de 2023

Security Hub CSPM está disponible en Oriente Medio (EAU)	Security Hub CSPM ya está disponible en Oriente Medio (EAU). Algunos controles tienen límites regionales.	12 de enero de 2023
Se agregó la integración de terceros con MetricStream	Security Hub CSPM ahora admite la integración de terceros MetricStream en todas las regiones, excepto China y. AWS GovCloud (US)	11 de enero de 2023
Se ha incrementado el límite de cuentas organizativas	El CSPM de Security Hub ahora admite hasta 11 000 cuentas de miembros por cada cuenta de administrador de CSPM de Security Hub por región.	27 de diciembre de 2022
ElasticBeanstalk3. Revertido	Security Hub CSPM anuló el control [ElasticBeanstalk. 3] Elastic Beanstalk debería transmitir los registros desde el estándar FSBP en todas CloudWatch las regiones.	21 de diciembre de 2022
Security Hub (CSPM) añade nuevos controles de seguridad	Los nuevos controles CSPM de Security Hub están disponibles para los clientes que hayan activado el estándar FSBP. Algunos controles tienen restricciones regionales .	15 de diciembre de 2022

[Guía sobre las próximas características](#)

Security Hub CSPM planea lanzar dos nuevas funciones : vista de controles consolidada y hallazgos de control consolidados. Estas próximas características pueden afectar los flujos de trabajo existentes que dependen del control de campos y valores de búsqueda.

9 de diciembre de 2022

[La integración con Amazon Security Lake ya está disponible](#)

Security Lake ahora se integra con el Security Hub CSPM al recibir las conclusiones del Security Hub CSPM.

29 de noviembre de 2022

[Support for Service-Managed Standard: AWS Control Tower](#)

Security Hub CSPM admite un nuevo estándar de seguridad denominado Service-Managed Standard: AWS Control Tower. AWS Control Tower gestiona este estándar.

28 de noviembre de 2022

[CIS AWS Foundations Benchmark v1.4.0 ya está disponible en las regiones de China](#)

Security Hub CSPM ahora es compatible con CIS AWS Foundations Benchmark v1.4.0 en las regiones de China.

18 de noviembre de 2022

[Ya está disponible la integración con Jira Service Management Cloud](#)

Jira Service Management Cloud ahora recibe los resultados del CSPM de Security Hub en todas las regiones disponibles, excepto en las regiones de China.

17 de noviembre de 2022

[AWS IoT Device Defender la integración ya está disponible](#)

AWS IoT Device Defender ahora envía los resultados al Security Hub CSPM en todas las regiones disponibles.

17 de noviembre de 2022

[Support para CIS AWS Foundations Benchmark v1.4.0](#)

Security Hub CSPM ahora proporciona controles de seguridad compatibles con CIS AWS Foundations Benchmark v1.4.0. Este estándar está disponible en todas las regiones disponibles, excepto en las regiones de China.

9 de noviembre de 2022

[Support for Security Hub \(anuncios de CSPM\) en AWS GovCloud \(US\)](#)

Ahora puede suscribirse a los anuncios de Security Hub CSPM con Amazon Simple Notification Service (Amazon SNS) AWS GovCloud en (EE. UU. Este) AWS GovCloud y (EE. UU. Oeste) para recibir notificaciones sobre Security Hub CSPM.

3 de octubre de 2022

[AWS Security Hub Cloud Security Posture Management \(CSPM\) añade un nuevo control de seguridad](#)

El nuevo Security Hub CSPM control AutoScaling.9 está disponible para los clientes que hayan activado el estándar FSBP. Los controles pueden tener [restricciones regionales](#).

1 de septiembre de 2022

<u>Suscríbase a los anuncios de Security Hub CSPM</u>	Ahora puede suscribirse a los anuncios de Security Hub CSPM con Amazon Simple Notification Service (Amazon SNS) para recibir notificaciones sobre Security Hub CSPM.	29 de agosto de 2022
<u>Expansión regional para la agregación entre regiones</u>	La agregación entre regiones ya está disponible para obtener resultados, actualizaciones de búsquedas y resultados en AWS GovCloud (US).	2 de agosto de 2022
<u>Nuevas integraciones de productos de terceros</u>	Fortinet: FortiCNP es una integración de terceros que recibe las conclusiones de Security Hub CSPM y JFrog es una integración de terceros que envía las conclusiones a Security Hub CSPM.	26 de julio de 2022
<u>EC2.27 está retirado</u>	Security Hub CSPM ha retirado la versión EC2.27: EC2 Las instancias en ejecución no deberían usar pares de claves, un control anterior del estándar AWS Foundational Security Best Practices (FSBP).	20 de julio de 2022

[Lambda.2 ya no es compatible con python3.6](#)

El CSPM de Security Hub ya no admite python3.6 como parámetro para Lambda.2

- Las funciones de Lambda deben usar tiempos de ejecución compatibles, un control del estándar Foundational Security Best Practices (FSBP). AWS

19 de julio de 2022

[AWS Security Hub Cloud Security Posture Management \(CSPM\) añade nuevos controles de seguridad](#)

Los nuevos controles CSPM de Security Hub están disponibles para los clientes que hayan activado el estándar FSBP. Algunos controles tienen [restricciones regionales](#).

22 de junio de 2022

[AWS Security Hub Cloud Security Posture Management \(CSPM\) apoya una nueva región](#)

Security Hub CSPM ya está disponible en Asia Pacífico (Yakarta). Algunos controles no están disponibles en esta región.

7 de junio de 2022

[Integración mejorada entre AWS Security Hub Cloud Security Posture Management \(CSPM\) y AWS Config](#)

Los usuarios de Security Hub CSPM pueden ver los resultados de las evaluaciones de AWS Config reglas como hallazgos en Security Hub CSPM.

6 de junio de 2022

<u>Se agregó la posibilidad de excluirse de los estándares de activación automática</u>	Para los usuarios que se han integrado con AWS Organizations, esta función les permite iniciar sesión en la cuenta de administrador CSPM de Security Hub y excluir las cuentas de nuevos miembros según los estándares de activación automática.	25 de abril de 2022
<u>Agregación entre regiones ampliada</u>	Se incluyó la agregación entre regiones para controlar los estados y las puntuaciones de seguridad.	20 de abril de 2022
<u>CompanyName y ahora ProductName son atributos de primer nivel</u>	Se agregaron nuevos atributos de nivel superior para establecer los nombres de las empresas y los productos asociados a las integraciones personalizadas	1 de abril de 2022
<u>Se agregaron nuevos controles al estándar de mejores prácticas de seguridad AWS fundamentales</u>	Se agregaron 5 controles nuevos al estándar de mejores prácticas de seguridad AWS fundamentales.	31 de marzo de 2022
<u>Se agregaron nuevos objetos de detalles de recursos al ASFF</u>	Se agregó un AwsRdsDbSecurityGroup tipo de recurso al ASFF.	25 de marzo de 2022

Se agregaron detalles de recursos adicionales en el ASFF	Se agregaron detalles adicionales a AwsAutoScalingScalingGroup , AwsElbLoadBalancer , AwsRedshiftCluster , y AwsCodeBuildProject .	25 de marzo de 2022
Se agregaron nuevos controles al estándar de mejores AWS prácticas de seguridad fundamentales	Se agregaron 15 controles nuevos al estándar de mejores prácticas de seguridad AWS fundamentales.	16 de marzo de 2022
Se agregaron nuevos controles al estándar de mejores prácticas de seguridad AWS fundamental y al estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS)	Se agregaron nuevos controles para Amazon OpenSearch Service, Amazon RDS, Amazon EC2, Elastic Load Balancing y CloudFront al estándar AWS Foundational Security Best Practices . También se agregaron dos nuevos controles de OpenSearch servicio al PCI DSS.	15 de febrero de 2022
Se agregó un nuevo campo al ASFF	Se agregó un nuevo campo: Muestra.	26 de enero de 2022
Se agregó la integración con AWS Health	AWS Health utiliza la mensajería de service-to-service eventos para enviar las conclusiones al Security Hub CSPM.	19 de enero de 2022

[Se agregó la integración con AWS Trusted Advisor](#)

Trusted Advisor envía los resultados de sus comprobaciones al Security Hub CSPM a medida que el Security Hub CSPM detecta. Security Hub CSPM envía los resultados de sus comprobaciones de mejores prácticas de seguridad AWS fundamentales a Trusted Advisor.

18 de enero de 2022

[Objetos de detalles de recursos actualizados en el ASFF](#)

Se agregaron `MixedInstancesPolicy` y `AvailabilityZones` a `AwsAutoScalingAutoScalingGroup`. Se agregó `MetadataOptions` a `AwsAutoScalingLaunchConfiguration`. Se agregó `BucketVersioningConfiguration` a `AwsS3Bucket`.

20 de diciembre de 2021

[Salida actualizada de la documentación del ASFF](#)

Anteriormente, las descripciones de los atributos del ASFF figuraban en un solo tema. Cada objeto de nivel superior y cada objeto de detalles de recursos se encuentran ahora en su propio tema. El tema de sintaxis del ASFF contiene enlaces a esos temas.

20 de diciembre de 2021

[Se agregaron nuevos objetos de detalles de recursos a ASFF para AWS Network Firewall](#)

Para AWS Network Firewall, se agregaron los siguientes objetos de detalles de recursos: `AwsNetworkFirewall`, `Firewall`, `AwsNetworkFirewallPolicy`, `AwsNetworkFirewallRuleGroup`.

20 de diciembre de 2021

[Se agregó soporte para la nueva versión de Amazon Inspector](#)

El Security Hub CSPM está integrado con la nueva versión de Amazon Inspector y con Amazon Inspector Classic. Amazon Inspector envía los resultados al Security Hub (CSPM).

29 de noviembre de 2021

[Se modificó la gravedad de .19 EC2](#)

La gravedad de EC2 .19 (los grupos de seguridad no deben permitir el acceso sin restricciones a los puertos de alto riesgo) ha cambiado de alta a crítica.

17 de noviembre de 2021

[Nueva integración con Sonrai Dig](#)

Security Hub CSPM ahora ofrece una integración con Sonrai Dig. Sonrai Digmonitoreará los entornos de nube para identificar los riesgos de seguridad. Sonrai Digenvía los resultados al Security Hub CSPM.

12 de noviembre de 2021

[Comprobación actualizada de los controles CIS 2.1 y .1 CloudTrail](#)

Además de comprobar que hay al menos un CloudTrail sendero multirregional, los CIS 2.1 y CloudTrail .1 ahora también comprueban que el ExcludeManagementEventSources parámetro esté vacío en al menos uno de los senderos multirregionales CloudTrail .

9 de noviembre de 2021

[Se agregó mayor compatibilidad para puntos de conexión de VPC](#)

El CSPM de Security Hub ahora está integrado AWS PrivateLink y es compatible con los puntos finales de VPC.

3 de noviembre de 2021

[Se agregaron controles al estándar de mejores prácticas de AWS seguridad fundamentales](#)

Se agregaron nuevos controles para Elastic Load Balancing (ELB.2 y ELB.8) y AWS Systems Manager (SSM.4).

2 de noviembre de 2021

[Se agregaron puertos a la verificación para el control 1.9 EC2](#)

EC2.19 ahora también comprueba que los grupos de seguridad no permiten el acceso sin restricciones a los siguientes puertos: 3000 (marcos de desarrollo web Go, Node.js y Ruby), 5000 (marcos de desarrollo web de Python), 8088 (puerto HTTP heredado) y 8888 (puerto HTTP alternativo)

27 de octubre de 2021

[Se agregó la integración con Logz.io Cloud SIEM](#)

Logz.io es un proveedor de Cloud SIEM que proporciona una correlación avanzada de los datos de registro y eventos para ayudar a los equipos de seguridad a detectar, analizar y responder a las amenazas de seguridad en tiempo real. Logz.io recibe las conclusiones del Security Hub CSPM.

25 de octubre de 2021

[Se agregó soporte para la agregación entre regiones de resultados](#)

La agregación entre regiones le permite ver todos sus resultados sin tener que cambiar de región. Las cuentas de administrador eligen una región de agregación y las regiones vinculadas. Los resultados de la cuenta de administrador y sus cuentas de miembros se agregan de las regiones vinculadas a la región de agregación.

20 de octubre de 2021

[Objetos de detalles de recursos actualizados en el ASFF](#)

Se agregaron detalles del certificado de visor a `AwsCloudFrontDistribution`. Se agregaron detalles adicionales a `AwsCodeBuildProject`. Se agregaron atributos del equilibrador de carga a `AwsElbV2LoadBalancer`. Se agregó el identificador de la cuenta del propietario del bucket de S3 a `AwsS3Bucket`.

8 de octubre de 2021

[Se agregaron nuevos objetos de detalles de recursos al ASFF](#)

Se agregaron los siguientes nuevos objetos de detalles de recursos al ASFF: `AwsEc2VpcEndpointService`, `AwsEcrRepository`, `AwsEksCluster`, `AwsOpenSearchServiceDomain`, `AwsWafRateBasedRule`, `AwsWafRegionalRateBasedRule`, `AwsXrayEncryptionConfig`

8 de octubre de 2021

[Se eliminó el tiempo de ejecución obsoleto del control Lambda.2](#)

En el estándar AWS Foundational Security Best Practices, se eliminó el `dotnetcore2.1` tiempo de ejecución de [Lambda.2] Las funciones Lambda deberían usar tiempos de ejecución compatibles.

6 de octubre de 2021

<u>Nuevo nombre para la integración de Check Point</u>	La integración con Check Point Dome9 Arc ahora es Check Point Posture Management. CloudGuard El ARN de integración no ha cambiado.	1 de octubre de 2021
<u>Se eliminó la integración con Alcide</u>	Se interrumpe la integración con Alcide KAudit.	30 de septiembre de 2021
<u>Se ha modificado la gravedad de .19 EC2</u>	La gravedad de [EC2.19] Los grupos de seguridad no deberían permitir el acceso sin restricciones a los puertos de alto riesgo ha cambiado de media a alta.	30 de septiembre de 2021
<u>La integración con ahora AWS Organizations es compatible en las regiones de China</u>	La integración de Security Hub CSPM con Organizations ahora es compatible con China (Beijing) y China (Ningxia).	20 de septiembre de 2021
<u>Nueva AWS Config regla para los controles S3.1 y PCI.S3.6</u>	Tanto S3.1 como PCI.S3.6 comprueban que la configuración de bloqueo de acceso público de Amazon S3 esté habilitada. La AWS Config regla para estos controles se ha cambiado de a. s3-account-level-public-access-blocks s3-account-level-public-access-blocks-periodic	14 de septiembre de 2021

[Se eliminaron los tiempos de ejecución obsoletos del control Lambda.2](#)

En el estándar AWS Foundatio
nal Security Best Practices
, se eliminaron los tiempos
de ruby2.5 ejecución
nodejs10.x y los tiempos
de ejecución de [Lambda.2
] Las funciones Lambda
deberían utilizar tiempos de
ejecución compatibles.

13 de septiembre de 2021

[Se modificó la gravedad del control CIS 2.2](#)

En el estándar CIS AWS
Foundations Benchmark, la
gravedad de la versión 2.2. —
Asegúrese de que la validació
n del archivo de CloudTrai
l registro esté habilitada y
cambie de Baja a Media.

13 de septiembre de 2021

[Se actualizaron ECS.1, Lambda.2 y SSM.1 en el estándar Foundational Security Best Practices AWS](#)

En el estándar AWS Foundatio
nal Security Best Practices
, ECS.1 ahora tiene un
parámetro establecido en.
SkipInactiveTaskDe
finitions true Esto
garantiza que el control solo
compruebe las definicio
nes de tareas activas. Para
Lambda.2, se agregó Python
3.9 a la lista de tiempos de
ejecución. Ahora, SSM.1
comprueba tanto las instancia
s detenidas como las que
están en ejecución.

7 de septiembre de 2021

El control PCI.Lambda.2 ahora excluye los recursos de Lambda @Edge	En el estándar de Payment Card Industry Data Security (PCI DSS), el control PCI.Lambda.2 ahora excluye los recursos de Lambda @Edge.	7 de septiembre de 2021
Se agregó la integración con HackerOne Vulnerability Intelligence	Security Hub CSPM ahora ofrece una integración con HackerOne Vulnerability Intelligence. La integración envía los resultados al Security Hub CSPM.	7 de septiembre de 2021
Objetos de detalles de recursos actualizados en el ASFFF	Para <code>AwsKmsKey</code> , se agregó <code>KeyRotationStatus</code> . Para <code>AwsS3Bucket</code> , se agregaron <code>AccessControlList</code> , <code>BucketLoggingConfiguration</code> , <code>BucketNotificationConfiguration</code> , y <code>BucketWebsiteConfiguration</code> .	2 de septiembre de 2021
Se agregaron nuevos objetos de detalles de recursos al ASFF	Se agregaron los siguientes nuevos objetos de detalles de recursos al ASFF: <code>AwsAutoScalingLaunchConfiguration</code> , <code>AwsEc2VpnConnection</code> , y <code>AwsEcrContainerImage</code> .	2 de septiembre de 2021
Se agregaron detalles al objeto Vulnerabilities en el ASFF	En <code>Cvss</code> , se agregaron <code>Adjustments</code> y <code>Source</code> . En <code>VulnerablePackages</code> , se agregó la ruta del archivo y el administrador de paquetes.	2 de septiembre de 2021

[Systems Manager Explorer y su OpsCenter integración ahora son compatibles en las regiones de China](#)

El Security Hub CSPM se integra con SSM Explorer y ahora OpsCenter es compatible con China (Pekín) y China (Ningxia).

31 de agosto de 2021

[Retirar el control Lambda.4](#)

Security Hub CSPM retira el control [Lambda.4] Las funciones de Lambda deberían tener configurada una cola de mensajes sin salida. Cuando se retira un control, deja de mostrarse en la consola y Security Hub CSPM no lo comprueba.

31 de agosto de 2021

[Retirando la PCI. EC2.3. Control](#)

Security Hub (CSPM) retira el control [PCI]. EC2.3] Se deben eliminar los grupos EC2 de seguridad no utilizados. Cuando se retira un control, deja de mostrarse en la consola y Security Hub CSPM no lo comprueba.

27 de agosto de 2021

[Cambio en la forma en que Security Hub CSPM envía los resultados a las acciones personalizadas](#)

Al enviar los resultados a una acción personalizada, Security Hub CSPM ahora envía cada hallazgo en un evento diferente Security Hub Findings - Custom Action.

20 de agosto de 2021

[Se agregó un nuevo código de motivo de estado de cumplimiento para los tiempos de ejecución de Lambda personalizados](#)

Se agregó un nuevo LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE código de motivo de estado de cumplimiento. Este código de motivo indica que Security Hub CSPM no pudo realizar una comprobación con un entorno de ejecución de Lambda personalizado.

20 de agosto de 2021

[AWS Firewall Manager la integración ahora es compatible en las regiones de China](#)

La integración de Security Hub CSPM con Firewall Manager ahora es compatible en China (Pekín) y China (Ningxia).

19 de agosto de 2021

[Nuevas integraciones con Caveonix Cloud y Forcepoint Cloud Security Gateway](#)

Security Hub CSPM ahora ofrece integraciones con y. Caveonix Cloud Forcepoint Cloud Security Gateway Ambas integraciones envían los resultados a Security Hub CSPM.

10 de agosto de 2021

[Se agregaron nuevos atributos
CompanyName , ProductName
y Region al ASFF](#)

Se agregaron los campos CompanyName , ProductName y Region al nivel superior del ASFF. Estos campos se rellenan automáticamente y, a excepción de las integraciones de productos personalizadas, no se pueden actualizar con BatchImportFindings o BatchUpdateFindings . En la consola, los filtros de búsqueda utilizan estos nuevos campos. En la API, los filtros CompanyName y ProductName usan los atributos que se encuentran debajo de ProductFields .

23 de julio de 2021

[Se agregaron y actualizaron
los objetos de detalles de los
recursos en el ASFF](#)

Se agregaron nuevos AwsRdsEventSubscription tipos de recursos y nuevos detalles de recursos. Se agregaron detalles del recurso para el tipo de recurso AwsEcsService . Se agregaron atributos al objeto de detalles del recurso AwsElasticsearchDomain .

23 de julio de 2021

[Se agregaron controles al estándar de mejores prácticas de AWS seguridad fundamentales](#)

Se han añadido nuevos controles para Amazon API Gateway (APIGateway.5), Amazon EC2 (EC2.19), Amazon ECS (ECS.2), Elastic Load Balancing (ELB.7), Amazon Service (ES.5 a ES.8), OpenSearch Amazon RDS (RDS.16 a RDS.23), Amazon Redshift (Redshift.4) y Amazon SQS (SQS.1).

20 de julio de 2021

[Se movió un permiso dentro de la política administrada de roles vinculados a un servicio](#)

Se trasladó el permiso `config:PutEvaluations` a la política `AWSSecurityHubServiceRolePolicy`, gestionada para que se aplique a todos los recursos.

14 de julio de 2021

[Se agregaron controles al estándar básico de mejores prácticas de seguridad AWS](#)

Se han añadido nuevos controles para Amazon API Gateway (APIGateway.4), Amazon CloudFront (CloudFront.5 y CloudFront.6), Amazon EC2 (EC2.17 y EC2.18), Amazon ECS (ECS.1), Amazon Service (ES.4), (IAM.21), OpenSearch Amazon RDS AWS Identity and Access Management (RDS.15) y Amazon S3 (S3.8).

8 de julio de 2021

[Se agregaron nuevos códigos de motivo de estado de cumplimiento para los resultados de control](#)

INTERNAL_SERVICE_ERROR indica que se ha producido un error desconocido. SNS_TOPIC_CROSS_ACCOUNT indica que el tema de SNS pertenece a una cuenta diferente. SNS_TOPIC_INVALID indica que el tema de SNS asociado no es válido.

6 de julio de 2021

[Se agregó la integración con Amazon Q Developer en las aplicaciones de chat](#)

Se agregó la integración con Amazon Q Developer en las aplicaciones de chat. Security Hub CSPM envía los resultados al desarrollador de Amazon Q en aplicaciones de chat.

30 de junio de 2021

[Se agregó un nuevo permiso a la política de administración de funciones vinculadas al servicio](#)

Se agregó un nuevo permiso a la política administrada AWSSecurityHubServiceRolePolicy para permitir que la función vinculada al servicio entregue los resultados de la evaluación a AWS Config.

29 de junio de 2021

[El recurso nuevo y actualizado detalla los objetos en el ASFF](#)

Se agregaron nuevos objetos de detalles de recursos para los clústeres de ECS y las definiciones de tareas de ECS. Se actualizó el objeto de la EC2 instancia para enumerar las interfaces de red asociadas. Se agregó el ID de certificado del cliente para las etapas V2 de API Gateway. Se agregó la configuración del ciclo de vida de los buckets S3.

24 de junio de 2021

[Se actualizó el cálculo de los estados de control agregados y las puntuaciones de seguridad estándar](#)

Security Hub CSPM ahora calcula el estado de control general y la puntuación de seguridad estándar cada 24 horas. En el caso de las cuentas de administrador, la puntuación ahora refleja si cada control está activado o desactivado para cada cuenta.

23 de junio de 2021

[Información actualizada sobre la gestión de cuentas suspendidas por Security Hub \(CSPM\)](#)

Se agregó información sobre cómo Security Hub CSPM gestiona las cuentas suspendidas. AWS

23 de junio de 2021

[Se agregaron pestañas para mostrar los controles habilitados y deshabilitados de la cuenta de administrador individual](#)

En el caso de la cuenta de administrador, las pestañas principales de la página de detalles estándar contienen información agregada de todas las cuentas. En las nuevas pestañas Habilitada para esta cuenta y Deshabilitada para esta cuenta se muestran las cuentas que están habilitadas o deshabilitadas para la cuenta de administrador individual.

23 de junio de 2021

[Se agregó java8.a12 a los parámetros de Lambda.2](#)

En el estándar AWS Foundational Security Best Practices, se agregó java8.a12 a los tiempos de ejecución compatibles con el control. Lambda.2

8 de junio de 2021

[Nuevas integraciones con Cyber Investigator de MicroFocus ArcSight NETSCOUT](#)

Se agregaron integraciones con NETSCOUT Cyber MicroFocus ArcSight Investigator. MicroFocus ArcSight recibe las conclusiones de Security Hub CSPM. El Cyber Investigator de NETSCOUT envía los resultados al Security Hub CSPM.

7 de junio de 2021

[Se agregaron detalles para AWSSecurityHubServiceRolePolicy](#)

Se actualizó la sección de políticas administradas para añadir detalles de la política administrada existente AWSSecurityHubServiceRolePolicy , que utiliza el rol vinculado al servicio CSPM de Security Hub.

4 de junio de 2021

[Nueva integración con Jira Service Management](#)

El conector AWS de administración de servicios de Jira envía las conclusiones a Jira y las utiliza para crear problemas con Jira. Cuando se actualizan los problemas de Jira, también se actualizan las conclusiones correspondientes en Security Hub CSPM.

26 de mayo de 2021

[Se actualizó la lista de controles compatibles para la región de Asia-Pacífico \(Osaka\)](#)

Se actualizaron el estándar CIS AWS Foundations y el estándar de seguridad de datos del sector de tarjetas de pago (PCI DSS) para indicar los controles que no son compatibles en Asia Pacífico (Osaka).

21 de mayo de 2021

[Nueva integración con Sysdig Secure para la nube](#)

Se agregó una integración con Sysdig Secure para la nube. La integración envía los resultados al Security Hub CSPM.

14 de mayo de 2021

[Se agregaron controles al estándar de AWS mejores prácticas de seguridad fundamentales](#)

Se han añadido nuevos controles para Amazon API Gateway (APIGateway.2 y APIGateway .3), AWS CloudTrail (CloudTrail.4 y CloudTrail .5), Amazon EC2 (EC2.15 y EC2 .16), (ElasticBeanstalk.1 y ElasticBeanstalk .2), AWS Elastic Beanstalk (Lambda.4), Amazon RDS AWS Lambda (RDS.12 — RDS.14), Amazon Redshift (Redshift.7), (.3 y .4) y (WAF.1). AWS Secrets Manager SecretsManager SecretsManager AWS WAF

10 de mayo de 2021

[Actualizaciones GuardDuty y controles de Amazon RDS](#)

Se ha cambiado la gravedad de GuardDuty.1 y PCI.GuardDuty.1 de Media a Alta. Se agregó un databaseEngines parámetro a RDS.8.

4 de mayo de 2021

[Se agregaron nuevos detalles de recursos al ASFF](#)

EnResources.Details , se agregaron nuevos objetos de detalles de recursos para la EC2 red de Amazon ACLs, EC2 las subredes de Amazon y AWS Elastic Beanstalk los entornos.

3 de mayo de 2021

[Se han añadido campos de consola para proporcionar valores de filtro para EventBridge las reglas de Amazon](#)

Los nuevos patrones de filtro predefinidos para EventBridge las reglas CSPM de Security Hub proporcionan campos de consola que puede usar para especificar valores de filtro.

30 de abril de 2021

[Se agregó la integración con Explorer y AWS Systems Manager OpsCenter](#)

Security Hub CSPM ahora admite una integración con Systems Manager Explorer y. OpsCenter La integración recibe las conclusiones del Security Hub CSPM y las actualiza en Security Hub CSPM.

26 de abril de 2021

[Nuevo tipo de integraciones de productos](#)

Un nuevo tipo de integración, UPDATE_FINDINGS_IN_SECURITY_HUB, indica que la integración de un producto actualiza los hallazgos que recibe de Security Hub CSPM.

22 de abril de 2021

[Se cambió "cuenta maestra" a "cuenta de administrador"](#)

Se ha cambiado el término "cuenta maestra" por "cuenta de administrador". El término también se cambia en la consola CSPM y la API de Security Hub.

22 de abril de 2021

Se actualizó la versión APIGateway 1.1 para reemplazar HTTP por Websocket	Se actualizaron el título, la descripción y la corrección de APIGateway .1. El control ahora comprueba el registro de ejecución de la API de Websocket en lugar del registro de ejecución de la API HTTP.	9 de abril de 2021
GuardDuty La integración de Amazon ahora es compatible en Beijing y Ningxia	La integración de Security Hub CSPM ahora GuardDuty es compatible en las regiones de China (Beijing) y China (Ningxia).	5 de abril de 2021
Se agregó node.js14.x a los tiempos de ejecución compatibles con el control Lambda.2	El control Lambda.2 del estándar de prácticas recomendadas de seguridad fundamentales ahora es compatible con el tiempo de ejecución node.js14.x .	30 de marzo de 2021
Lanzamiento del Security Hub CSPM en Asia Pacífico (Osaka)	Security Hub CSPM ya está disponible en la región de Asia Pacífico (Osaka).	29 de marzo de 2021
Se agregaron campos de búsqueda de proveedores a la de resultado de detalles	En el panel de detalles de búsqueda, la nueva sección Búsqueda de campos de proveedores contiene los valores de confianza, criticidad, resultados relacionados, gravedad y tipos de proveedor .	24 de marzo de 2021

[Se agregó la opción de recibir resultados confidenciales de Amazon Macie](#)

La integración con Macie ahora se puede configurar para enviar los hallazgos confidenciales al Security Hub CSPM.

23 de marzo de 2021

[¿Está realizando la transición a la administración de cuentas? AWS Organizations](#)

Para los clientes que ya tienen una cuenta de administrador con cuentas de miembros, se agregó nueva información sobre cómo pasar de administrar cuentas mediante invitación a administrar cuentas mediante Organizations.

22 de marzo de 2021

[Nuevos objetos en el ASFF para obtener información sobre la configuración de bloques de acceso público de Amazon S3](#)

En Resources , un nuevo tipo de AwsS3AccountPublicAccessBlock recurso y un objeto de detalles proporcionan información sobre la configuración del bloque de acceso público de Amazon S3 para las cuentas. En el objeto de detalles del recurso AwsS3Bucket , el objeto PublicAccessBlockConfiguration proporciona la configuración del bloque de acceso público para el bucket S3.

18 de marzo de 2021

[Nuevo objeto en el ASFF que permite buscar proveedor para actualizar campos específicos](#)

El nuevo objeto `FindingProviderFields` del ASFF se utiliza en `BatchImportFindings` para proporcionar valores para `Confidence`, `Criticality`, `RelatedFindings`, `Severity`, y `Types`. Los campos originales solo deben actualizarse utilizando `BatchUpdateFindings`.

18 de marzo de 2021

[Nuevo `DataClassification` objeto para los recursos en el ASFF](#)

El nuevo `Resources.DataClassification` objeto del ASFF se utiliza para proporcionar información sobre los datos confidenciales que se detectaron en el recurso.

18 de marzo de 2021

[Valor `CONFIG\_REURNS\_NOT\_APPLICABLE` agregado a los códigos de estado de cumplimiento disponibles](#)

Para el estado de cumplimiento `NOT_AVAILABLE`, se eliminó el código de motivo `RESOURCE_NO_LONGER_EXISTS` y se agregó el código de motivo `CONFIG_REURNS_NOT_APPLICABLE`.

16 de marzo de 2021

[Nueva política gestionada para la integración con AWS Organizations](#)

Una nueva política gestionada proporciona a las Organizaciones los permisos que necesitan la cuenta de administración de la organización y la cuenta de administrador CSPM de Security Hub delegada. `AWSSecurityHubOrganizationsAccess`

15 de marzo de 2021

[La información sobre las políticas gestionadas y las funciones vinculadas a los servicios se trasladó al capítulo de seguridad](#)

La información sobre las políticas gestionadas se revisa y amplía. Tanto la información sobre las políticas gestionadas como la información sobre las funciones vinculadas a los servicios se han trasladado al capítulo de seguridad.

15 de marzo de 2021

[Nueva integración con DB SecureCloud](#)

Se agregó SecureCloud DB a la lista de integraciones de terceros. SecureCloudDB es una herramienta de seguridad de bases de datos nativa de la nube que proporciona una visibilidad completa de las posturas y actividades de seguridad internas y externas. SecureCloudDB envía los resultados al Security Hub CSPM.

4 de marzo de 2021

[Se revisó la gravedad de los controles CIS 1.1 y CIS 3.1 – CIS 3.14](#)

La gravedad de los controles CIS 1.1 y CIS 3.1 – CIS 3.14 se cambia a Baja.

3 de marzo de 2021

<u>Se eliminó el control RDS.11</u>	Se eliminó el control RDS.11 del estándar de prácticas recomendadas de seguridad fundamentales.	3 de marzo de 2021
<u>Integración actualizada para Turbot</u>	La integración de Turbot se actualizó para enviar y recibir resultados.	26 de febrero de 2021
<u>Se agregaron controles al estándar de prácticas recomendadas de seguridad fundamentales</u>	Se han añadido nuevos controles para Amazon API Gateway (APIGateway.1), Amazon EC2 (EC2.9 y EC2.10), Amazon Elastic File System (EFS.2), Amazon OpenSearch Service (ES.2 y ES.3), Elastic Load Balancing (ELB.6) y () (KMS.3). AWS Key Management Service AWS KMS	11 de febrero de 2021
<u>Se agregó un filtro ProductArn opcional a la DescribeProducts API</u>	La operación DescribeProducts de API ahora incluye un parámetro ProductArn opcional. El parámetro ProductArn se utiliza para identificar la integración específica de producto para la que se devolverán los detalles.	3 de febrero de 2021
<u>Nueva integración con Antivirus para Amazon S3 de Cloud Storage Security</u>	La integración con Antivirus para Amazon S3 envía los resultados del análisis de virus al Security Hub (CSPM) como resultados.	27 de enero de 2021

[Se actualizó el proceso de cálculo de la puntuación de seguridad de las cuentas de administrador](#)

Para una cuenta de administrador, Security Hub CSPM utiliza un proceso independiente para calcular la puntuación de seguridad. El nuevo proceso garantiza que la puntuación incluya controles que estén habilitados para las cuentas de miembros, pero deshabilitados para la cuenta de administrador.

21 de enero de 2021

[Nuevos campos y objetos en el ASFF](#)

Se agregó un nuevo Action objeto para rastrear las acciones que se produjeron contra un recurso. Se agregaron campos al AwsEc2NetworkInterface objeto para rastrear los nombres de DNS y las direcciones IP. Se agregó un objeto AwsSsmPatchCompliance nuevo a los detalles del recurso.

21 de enero de 2021

[Se agregaron controles al estándar de prácticas recomendadas de seguridad fundamentales](#)

Se agregaron nuevos controles para Amazon CloudFront (CloudFront.1 a CloudFront .4), Amazon DynamoDB (DynamoDB .1 a DynamoDB.3), Elastic Load Balancing (ELB.3 a ELB.5), Amazon RDS (RDS.9 a RDS.11), Amazon Redshift (Redshift.1 a Redshift.3 y Redshift.6) y Amazon SNS (SNS.1).

15 de enero de 2021

[El estado del flujo de trabajo se restablece en función del estado del registro o del estado de cumplimiento](#)

Security Hub CSPM restablece automáticamente el estado del flujo de trabajo desde NOTIFIED o RESOLVED hasta NEW si se activa una búsqueda archivada, o si el estado de conformidad de una búsqueda cambia de PASSED a, oFAILED. WARNING NOT_AVAILABLE. Estos cambios indican que es necesaria una investigación adicional.

7 de enero de 2021

[Se agregó ProductFields información para los resultados basados en el control](#)

En el caso de las conclusiones que se generan a partir de los controles, se ha añadido información sobre el contenido del ProductFields objeto en el formato de comprobación de AWS seguridad (ASFF).

29 de diciembre de 2020

[Actualizaciones del hallazgo gestionado](#)

Se ha cambiado el título de hallazgo 5. Se agregó un nuevo hallazgo, 32, que comprueba si hay usuarios de IAM con actividades sospechosas.

22 de diciembre de 2020

[Actualizaciones de los controles IAM.7 y Lambda.1](#)

En el estándar AWS Foundational Security Best Practices, se actualizaron los parámetros del IAM.7. Se actualizaron el título y la descripción de Lambda.1.

22 de diciembre de 2020

[Integración ampliada con ITSM ServiceNow](#)

La integración de ServiceNow ITSM permite a los usuarios crear automáticamente incidentes o problemas cuando se recibe un hallazgo de CSPM de Security Hub. Las actualizaciones de estos incidentes o problemas dan lugar a actualizaciones de los hallazgos de Security Hub CSPM.

11 de diciembre de 2020

[Nueva integración con AWS Audit Manager](#)

Security Hub CSPM ahora ofrece una integración con AWS Audit Manager. La integración permite a Audit Manager recibir las conclusiones basadas en el control de Security Hub CSPM.

8 de diciembre de 2020

[Nueva integración con Aqua Security Kube-bench](#)

Security Hub CSPM agregó una integración con Aqua Security Kube-bench. La integración envía los resultados al Security Hub CSPM.

24 de noviembre de 2020

[Cloud Custodian ya está disponible en las regiones de China](#)

La integración con Cloud Custodian ya está disponible en las regiones de China (Pekín) y China (Ningxia).

24 de noviembre de 2020

[BatchImportFindings ahora se puede usar para actualizar campos adicionales](#)

Anteriormente, no se podía utilizar BatchImportFindings para actualizar los campos Confidence , Criticality , RelatedFindings , Severity, y Types. Ahora, si estos campos no se han actualizado con BatchUpdateFindings , se pueden actualizar con BatchImportFindings . Una vez actualizados por BatchUpdateFindings , no se pueden actualizar por BatchImportFindings .

24 de noviembre de 2020

[Security Hub CSPM ahora está integrado con AWS Organizations](#)

Los clientes ahora pueden administrar las cuentas de los miembros mediante la configuración de sus cuentas de Organizations (Organizaciones). La cuenta de administración de la organización designa la cuenta de administrador CSPM de Security Hub, que determina qué cuentas de la organización se deben habilitar en Security Hub CSPM. El proceso de invitación manual se puede seguir utilizando para las cuentas que no forman parte de una organización.

23 de noviembre de 2020

[Se ha eliminado el formato de lista de resultados independiente para los controles de gran volumen](#)

La lista de resultados de un control ya no utiliza el formato de página Resultados cuando hay un gran número de resultados.

19 de noviembre de 2020

[Integraciones de terceros nuevas y actualizadas](#)

Security Hub CSPM ahora admite integraciones con cloudtamer.io, 3CORESec, Prowler y Kubernetes Security. StackRox QRadar IBM ya no envía los resultados. Solo recibe los resultados.

30 de octubre de 2020

[Se agregó la opción de descargar la lista de resultados desde la página de detalles del control.](#)

En la página de detalles del control, hay una nueva opción de Descargar que permite descargar la lista de resultados en un archivo.csv. La lista descargada respeta todos los filtros que estén en la lista. Si seleccionó resultados específicos, la lista descargada solo incluye esos resultados.

26 de octubre de 2020

[Se agregó la opción de descargar la lista de controles desde la página de detalles estándar.](#)

En la página de detalles estándar, hay una nueva opción de Descargar que permite descargar la lista de controles a un archivo.csv. La lista descargada respeta todos los filtros que estén en la lista. Si ha seleccionado un control específico, la lista descargada solo incluye ese control.

26 de octubre de 2020

[Integraciones de socios nuevas y actualizadas](#)

Security Hub CSPM ahora está integrado con. ThreatModeler Se han actualizado las siguientes integraciones de socios para que reflejen los nuevos nombres de sus productos. Twistlock Enterprise Edition ahora es Palo Alto Networks - Prisma Cloud Compute. También de Palo Alto Networks, Demisto ahora es Cortex XSOAR y Redlock ahora es Prisma Cloud Enterprise.

23 de octubre de 2020

Lanzamiento del Security Hub CSPM en China (Pekín) y China (Ningxia)	Security Hub CSPM ya está disponible en las regiones de China (Pekín) y China (Ningxia).	21 de octubre de 2020
Formato revisado para los atributos del ASFF y las integraciones de terceros	Las listas de atributos del ASFF y las integraciones de socios ahora utilizan un formato basado en listas en lugar de tablas. La sintaxis, los atributos y la taxonomía de tipos del ASFF se encuentran ahora en temas separados.	15 de octubre de 2020
Página de detalles estándar rediseñada	La página de detalles estándar de un estándar activado ahora muestra una lista de controles en pestañas. Las pestañas filtran la lista de controles en función del estado del control.	7 de octubre de 2020
Sustituyó Events por CloudWatch EventBridge	Se han sustituido las referencias a Amazon CloudWatch Events por Amazon EventBridge.	1 de octubre de 2020
Nuevas integraciones con Blue Hexagon para AWS las series VM de Alcide KAudit y Palo Alto Networks.	Security Hub CSPM ahora está integrado con Blue Hexagon for AWS, Alcide KAudit y Palo Alto Networks VM-Series. Blue Hexagon for AWS y KAudit envían los resultados a Security Hub CSPM. VM-Series recibe las conclusiones de Security Hub CSPM.	30 de septiembre de 2020

[El recurso nuevo y actualizado detalla los objetos en el ASFF](#)

Se agregaron nuevos `Resources.Details` objetos para `AwsApiGatewayRestApi` , `AwsApiGatewayStage` , `AwsApiGatewayV2Api` , `AwsApiGatewayV2Stage` , `AwsCertificateManagerCertificate` , `AwsElasticLoadBalancer` , `AwsIAMGroup` , y `AwsRedshiftCluster` . Se agregaron detalles a los objetos `AwsCloudFrontDistribution` , `AwsIAMRole` y `AwsIAMAccessKey` .

30 de septiembre de 2020

[Nuevo ResourceRole atributo para los recursos en el ASFF para rastrear si un recurso es un actor o un objetivo.](#)

El `ResourceRole` atributo de los recursos indica si el recurso es el objetivo de la actividad de búsqueda o el autor de la actividad de búsqueda. Los valores válidos son `ACTOR` y `TARGET`.

30 de septiembre de 2020

[Se agregó AWS Systems Manager Patch Manager a las integraciones de servicios disponibles AWS](#)

AWS Systems Manager Patch Manager ahora está integrado con Security Hub CSPM. Patch Manager envía los resultados al Security Hub CSPM cuando las instancias de la flota de un cliente no cumplen con su estándar de cumplimiento de parches.

22 de septiembre de 2020

[Se agregaron nuevos controles al estándar de AWS mejores prácticas de seguridad fundamentales](#)

Se han añadido nuevos controles para los siguientes servicios: Amazon EC2 (EC2.7 y EC2 .8), Amazon EMR (EMR.1), IAM (IAM.8), Amazon RDS (RDS.4 a RDS.8), Amazon S3 (S3.6) y (.1 y .2). AWS Secrets Manager SecretsManager SecretsManager

15 de septiembre de 2020

[Nuevas claves de contexto para la política de IAM para controlar el acceso a los BatchUpdateFindings campos](#)

Las políticas de IAM ahora se pueden configurar para restringir el acceso a los campos y a sus valores durante su uso BatchUpdateFindings .

10 de septiembre de 2020

[Acceso ampliado a BatchUpdateFindings las cuentas de los miembros](#)

Por defecto, las cuentas de miembros ahora tienen el mismo acceso a BatchUpdateFindings que las cuentas de administrador.

10 de septiembre de 2020

[Nuevos controles AWS KMS incluidos en el estándar fundamental de mejores prácticas de seguridad](#)

Se agregaron dos controles nuevos (KMS.1 y KMS.2) al estándar de prácticas recomendadas de seguridad fundamentales. Los nuevos controles comprueban si las políticas de IAM restringen el acceso a las acciones de AWS KMS descifrado.

9 de septiembre de 2020

[Se eliminaron los resultados de los controles a nivel de cuenta](#)

Security Hub CSPM ya no genera hallazgos a nivel de cuenta para un control. Solo se generan resultados a nivel de recursos.

1 de septiembre de 2020

[Nuevo PatchSummary objeto en el ASFF](#)

Se agregó el PatchSummary objeto al ASFF. El PatchSummary objeto proporciona información sobre el cumplimiento de los parches de un recurso en relación con un estándar de cumplimiento seleccionado.

1 de septiembre de 2020

[Página de detalles de control rediseñada](#)

Se ha rediseñado la página de detalles de los controles. La lista de búsqueda de controles incluye pestañas que permiten filtrar rápidamente la lista en función del estado de cumplimiento. También puede ver rápidamente los resultados excluidos. Cada entrada proporciona acceso a detalles adicionales sobre el recurso de búsqueda, la AWS Config regla y las notas de búsqueda.

28 de agosto de 2020

[Nuevas opciones de filtro para los resultados](#)

Para buscar filtros, puede usar el filtro no es para buscar resultados en los que el valor de un campo no sea igual al valor del filtro. Puede utilizar el campo no empieza por para encontrar resultados en los que un valor de campo no comience por el valor de filtro especificado.

28 de agosto de 2020

[El nuevo recurso detalla los objetos en el ASFF](#)

Se agregaron nuevos `Resources.Details` objetos para los siguientes tipos de recursos: `AwsDynamoDbTable` , `AwsEc2Eip` , `AwsIamPolicy` , `AwsIamUser` , `AwsRdsDbCluster` , `AwsRdsDbClusterSnapshot` , `AwsRdsDbSnapshot` , `AwsSecretsManagerSecret`

18 de agosto de 2020

[Nueva integración con RSA Archer](#)

Security Hub CSPM ahora está integrado con RSA Archer. RSA Archer recibe las conclusiones del Security Hub CSPM.

18 de agosto de 2020

[Nuevo campo de descripción para AwsKmsKey](#)

Se agregó un `Description` campo al `AwsKmsKey` objeto situado abajo de `Resources.Details` .

18 de agosto de 2020

[Se agregaron campos a AwsRdsDbInstance](#)

Se agregaron varios atributos al `AwsRdsDbInstance` objeto que se encuentra abajo de `Resources.Details`.

18 de agosto de 2020

[Se actualizó la forma en que Security Hub \(CSPM\) determina el estado general de un control.](#)

En el caso de los controles que no encuentran resultados, el estado es Sin datos en lugar de Desconocido. El estado del control incluye los resultados a nivel de cuenta y a nivel de recursos. El estado de control no utiliza el estado del flujo de trabajo de los resultados, excepto para ignorar los resultados excluidos.

13 de agosto de 2020

[Se actualizó la forma en que Security Hub CSPM calcula la puntuación de seguridad de un estándar](#)

Al calcular la puntuación de seguridad de un estándar, Security Hub CSPM ahora ignora los controles con el estado Sin datos. La puntuación de seguridad es la proporción entre los controles aprobados y los controles activados, excluyendo los controles sin datos.

13 de agosto de 2020

[Nueva opción para habilitar automáticamente nuevos controles en los estándares habilitados](#)

Se agregó una opción a Configuración para habilitar automáticamente los nuevos controles en los estándares que estén habilitados. También puede utilizar la operación de la API `UpdateSecurityHubConfiguration` para configurar esta opción.

31 de julio de 2020

[Nuevos controles para el estándar de Payment Card Industry Data Security Standard \(PCI DSS\)](#)

Se agregaron nuevos controles al estándar PCI DSS. Los identificadores de los nuevos controles son PCI.DMS.1 y PCI. EC25., PCI. EC26., PCI. ELBV21., PCI. GuardDuty1., PCI.IAM.7, PCI.IAM.8, PCI.3.5, PCI.S3.6, PCI. SageMaker.1, PCI.SSM.2 y PCI.SSM.3.

29 de julio de 2020

[Controles nuevos y actualizados para el estándar de prácticas recomendadas de seguridad fundamentales](#)

Se agregaron nuevos controles al estándar fundamental de mejores prácticas de seguridad. Los identificadores de los nuevos controles son AutoScaling .1, DMS.1, .4, .6, S3.5 y SSM.3. EC2 EC2 Se actualizó el título de ACM.1 y se cambió el valor del parámetro `daysToExpiration` a 30.

29 de julio de 2020

Nuevo Vulnerabilities objeto en el ASFF	Se agregó el objeto <code>Vulnerabilities</code> , que proporciona información sobre las vulnerabilidades asociadas al resultado.	1 de julio de 2020
Nuevos Resource.Details objetos en el ASFF para grupos, EC2 volúmenes y EC2 VPCs	Se agregaron los objetos <code>AwsAutoScalingAutoScalingGroup</code> , <code>AWSEc2Volume</code> , y <code>AwsEc2Vpc</code> a <code>Resource.Details</code> .	1 de julio de 2020
Nuevo NetworkPath objeto en el ASFF	Se agregó el <code>NetworkPath</code> objeto, que proporciona información sobre una ruta de red relacionada con el resultado.	1 de julio de 2020
Resuelva automáticamente los resultados cuando Compliance.Status es PASSED	Para los hallazgos de los controles, si <code>Compliance.Status</code> es así <code>PASSED</code> , el Security Hub CSPM se establece <code>Workflow.Status</code> automáticamente en. <code>RESOLVED</code>	24 de junio de 2020
AWS Command Line Interface ejemplos	Se agregaron ejemplos y AWS CLI sintaxis para varias tareas de CSPM de Security Hub. Incluye habilitar el CSPM de Security Hub, administrar información, administrar estándares y controles , administrar integraciones de productos y deshabilitar Security Hub CSPM.	24 de junio de 2020

<u>Nuevo Severity. Original atributo en el ASFF</u>	Se agregó el atributo <code>Severity.Original</code> , que es la gravedad original del proveedor de resultados. Esto reemplaza al atributo <code>Severity.Product</code> que ha quedado obsoleto.	20 de mayo de 2020
<u>Nuevo Compliance. StatusReasons objeto en el ASFF para obtener detalles sobre el estado de un control</u>	Se agregó el objeto <code>Compliance.StatusReasons</code> , que proporciona contexto adicional para el estado actual de un control.	20 de mayo de 2020
<u>Nuevo estándar fundament al de mejores prácticas de seguridad AWS</u>	Se agregó el nuevo estándar AWS fundamental de mejores prácticas de seguridad, que consiste en un conjunto de controles que detectan si las cuentas y los recursos implementados se desvían de las mejores prácticas de seguridad.	22 de abril de 2020
<u>Nueva opción de consola para actualizar el estado de flujo de trabajo para un resultado</u>	Se agregó información sobre el uso de la consola o la API de Security Hub para establecer el estado de flujo de trabajo para los hallazgos.	16 de abril de 2020

[Nueva BatchUpdateFindings API para actualizaciones de cliente según los resultados](#)

Se agregó información sobre el uso de BatchUpdateFindings para actualizar información relacionada con el proceso de investigación de un hallazgo. BatchUpdateFindings reemplaza a UpdateFindings , que está obsoleto.

16 de abril de 2020

[Actualizaciones del formato de búsqueda AWS de seguridad \(ASFF\)](#)

Se agregaron varios tipos de recursos nuevos. Se agregó un nuevo atributo Label al objeto Severity. Label está destinado a reemplazar el campo Normalized . Se agregó un nuevo objeto Workflow para realizar un seguimiento del proceso de una investigación sobre un hallazgo. Workflow contiene un atributo Status, que reemplaza el atributo Workflowstate existente.

12 de marzo de 2020

[Actualizaciones a la página Integraciones](#)

Actualizado para reflejar los cambios realizados en la página Integrations (Integraciones). Para cada integración, la página ahora muestra la categoría de integración y si cada integración envía o recibe las conclusiones de Security Hub CSPM. También proporciona los pasos específicos necesarios para habilitar cada integración.

26 de febrero de 2020

[Nuevas integraciones de productos de terceros](#)

Se agregaron las siguientes integraciones de productos nuevos: Cloud Custodian, FireEye Helix, Forcepoint CASB, Forcepoint DLP, Forcepoint NGFW, Rackspace Cloud Native Security y Vectra.ai Cognito Detect.

21 de febrero de 2020

[Nuevo estándar de seguridad para el Payment Card Industry Data Security Standard \(PCI DSS\)](#)

Se agregó el estándar de seguridad Security Hub CSPM para el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS). Cuando se habilita este estándar, el Security Hub CSPM realiza comprobaciones automatizadas de los controles relacionados con los requisitos de PCI DSS.

13 de febrero de 2020

Actualizaciones del formato de búsqueda de AWS seguridad (ASFF)	Se agregó un campo para los requisitos relacionados para los controles de estándares . Se agregaron nuevos tipos de recursos y nuevos detalles de recursos . El ASFF ahora también le permite proporcionar hasta 32 recursos.	5 de febrero de 2020
Nueva opción para desactivar los controles estándar de seguridad individuales	Se agregó información acerca de cómo controlar si cada control del estándar de seguridad individual está habilitado.	15 de enero de 2020
Actualizaciones de los conceptos de CSPM de Security Hub	Se actualizaron algunas descripciones y se agregaron nuevos términos a los conceptos de CSPM de Security Hub .	21 de septiembre de 2019
AWS Versión de disponibilidad general de Security Hub Cloud Security Posture Management (CSPM)	Actualizaciones de contenido para reflejar las mejoras realizadas en Security Hub CSPM durante el período beta.	25 de junio de 2019
Se agregaron pasos de corrección para las comprobaciones de CIS Foundations AWS	Se agregaron pasos de corrección a los estándares de seguridad compatibles con AWS Security Hub Cloud Security Posture Management (CSPM) .	15 de abril de 2019

[versión beta de AWS Security Hub Cloud Security Posture Management \(CSPM\)](#)

Publicó la versión beta de la Guía del usuario de AWS Security Hub Cloud Security Posture Management (CSPM).

18 de noviembre de 2018

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.