



Guía del usuario

AWS Security Hub



AWS Security Hub: Guía del usuario

Copyright © 2024 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
Ventajas de Security Hub	2
Acceso a Security Hub	3
Servicios relacionados	4
Prueba gratuita, uso y precios de Security Hub	4
Visualización de detalles de uso y costo estimado	5
Información sobre precios	5
Conceptos de Security Hub	6
Habilitación de Security Hub	13
Verificación de los permisos necesarios	13
Habilitación de la integración de Security Hub con Organizations	13
Configuración centralizada	14
Habilitación de manual de Security Hub	15
Script de habilitación de múltiples cuentas	17
Próximos pasos: gestión de la postura e integraciones	17
Configuración AWS Config para Security Hub	18
Consideraciones antes de habilitar y configurar AWS Config	18
Registrar los recursos en AWS Config	19
Formas de habilitar y configurar AWS Config	20
Control de configuración 1	21
Generación de reglas vinculadas a servicios	21
Consideraciones sobre costos	22
Configuración local	22
Configuración centralizada	23
Beneficios de usar la configuración centralizada	24
¿Cuándo se debe utilizar la configuración centralizada?	25
Términos y conceptos de la configuración centralizada	26
Habilitar la configuración centralizada	32
Administración centralizada frente a autoadministración	37
Funcionamiento de las políticas de configuración	42
Creación y asociación de políticas de configuración	48
Revisar el estado y los detalles de la política	54
Actualización de las políticas de configuración	58
Eliminación de políticas de configuración	63

Desasociación de una configuración	65
Configuración en contexto	67
Deshabilitación de la configuración centralizada	69
Administración de cuentas de administrador y de miembros	73
Administración de cuentas con AWS Organizations	73
Administración manual de cuentas mediante invitación	74
Recomendaciones para entornos de varias cuentas	75
Número máximo de cuentas miembro	75
Creación de relaciones administrador-miembro	75
Coordinar cuentas de administrador en todos los servicios	76
Administración de cuentas con Organizations	77
Integración de Security Hub con AWS Organizations	78
Habilitación automática de cuentas nuevas en Security Hub	87
Habilitación manual de Security Hub en cuentas nuevas	89
Desasociación de cuentas de la organización como cuentas de miembro	91
Administración de cuentas por invitación en Security Hub	93
Cómo agregar e invitar cuentas de miembro en Security Hub	95
Cómo responder a una invitación	99
Cómo desvincular las cuentas de miembro en Security Hub	102
Cómo eliminar cuentas de miembro en Security Hub	103
Desvincularse de una cuenta de administrador de Security Hub	105
Transición a AWS Organizations	106
Acciones permitidas en las cuentas de administrador y de miembro	108
Efecto de las acciones de la cuenta en los datos de Security Hub	114
Security Hub desactivado	114
Cuenta miembro disociada de la cuenta de administrador	115
La cuenta miembro se elimina de una organización	115
La cuenta está suspendida.	116
La cuenta se cierra	116
Agregación entre regiones	118
Tipos de datos que se agregan	119
Agregación de cuentas de administrador y de miembros	121
Configuración centralizada y agregación	122
Habilitación de agregación	123
Visualización de la configuración de agregación	125
Actualización de la configuración de agregación	127

Detención de la agregación	129
Para eliminar el agregador de resultados (consola)	129
Estándares	131
Referencia de estándares de Security Hub	132
AWS Mejores prácticas fundamentales de seguridad	133
Indicador de referencia de CIS AWS Foundations	149
NIST SP 800-53 Rev. 5	168
PCI DSS	184
AWS Estándar de etiquetado de recursos	195
Estándar de gestión de servicios	201
Habilitación de un estándar	216
Habilitación de un estándar en varias cuentas y regiones	217
Habilitación de un estándar en una sola cuenta y región	218
Desactivación de un estándar	219
Desactivación de un estándar en varias cuentas y regiones	219
Deshabilitación de un estándar en una sola cuenta y región	220
Desactivar los estándares con habilitación automática	222
Visualización de los detalles de un estándar	223
Descripción de la puntuación de seguridad del estándar	224
Visualización de los controles de un estándar habilitado	225
Controles	228
Vista de controles consolidados	228
Puntuación general de seguridad de los controles	229
Referencia de controles de Security Hub	230
Controles de Cuenta de AWS	360
Controles de Amazon API Gateway	362
AWS AppConfig controles	368
AppFlow Controles de Amazon	374
AWS App Runner controles	376
AWS AppSync controles	379
Controles de Amazon Athena	384
Controles de AWS Backup	389
AWS Batch controles	397
AWS Certificate Manager controles	402
Controles de AWS CloudFormation	406
CloudFront Controles de Amazon	409

AWS CloudTrail controles	419
Controles de Amazon CloudWatch	429
Controles de AWS CodeArtifact	477
AWS CodeBuild controles	478
Controles de Amazon CodGuru Profiler	484
Controles de Amazon CodGuru Reviewer	486
Controles de Amazon Cognito	488
AWS Config controles	489
Controles de Amazon Connect	492
Controles de Amazon Data Firehose	494
Controles de AWS DataSync	495
Controles de Amazon Detective	496
AWS DMS controles	498
Controles de Amazon DocumentDB	512
Controles de Amazon DynamoDB	517
EC2 Controles de Amazon	525
Controles EC2 de Amazon Auto Scaling	594
ECRControles de Amazon	603
ECSControles de Amazon	607
EFSControles de Amazon	621
EKSControles de Amazon	628
ElastiCache Controles de Amazon	635
AWS Elastic Beanstalk controles	641
Controles del equilibrador de carga elástico	644
Controles de Elasticsearch	659
Controles de Amazon EMR	668
EventBridge Controles de Amazon	672
Controles de Amazon Fraud Detector	675
FSxControles de Amazon	683
Controles de AWS Global Accelerator	685
AWS Glue controles	687
GuardDuty Controles de Amazon	689
AWS Identity and Access Management Controles (IAM)	701
Controles de Amazon Inspector	737
Controles de AWS IoT	741
AWS Controles de IoT Events	750

AWS SiteWise Controles de IoT	755
AWS TwinMaker Controles de IoT	763
AWS Controles IoT Wireless	770
Controles de Amazon IVS	775
Controles de Amazon Keyspaces	780
Amazon Kinesis Kinesis Kinesis Controles	782
AWS KMS controles	786
AWS Lambda controles	791
Controles de Amazon Macie	797
MSKControles de Amazon	799
Controles de Amazon MQ	802
Controles de Amazon Neptune	807
Controles de AWS Network Firewall	815
Controles OpenSearch de Amazon Service	824
AWS Private CA controles	835
Controles de Amazon RDS	837
Controles de Amazon Redshift	879
Controles de Amazon Route 53	895
Controles de Amazon S3	898
Controles de Amazon SageMaker AI	922
AWS Secrets Manager controles	926
Controles de AWS Service Catalog	933
Controles para Amazon Simple Email Service	934
SNSControles de Amazon	937
Controles de Amazon SQS	942
AWS Step Functions controles	944
AWS Systems Manager controles	947
AWS Transfer Family controles	951
AWS WAF controles	954
Controles de Amazon WorkSpaces	962
Permisos para configurar los controles	963
Habilitación de controles	964
Habilitación de un control en todos los estándares	965
Habilitación de un control en un estándar específico	968
Habilitación automática de nuevos controles	971
Deshabilitación de controles	973

Deshabilitar un control en todos los estándares	974
Deshabilitación de un control en un estándar específico	977
Controles sugeridos para deshabilitar	979
Controles y puntuaciones de seguridad	984
AWS Config Recursos necesarios para los hallazgos de control	985
Programación para ejecutar comprobaciones de seguridad	1038
Generación y actualización de los resultados de control	1039
Estado de conformidad y el estado de control	1054
Calcular las puntuaciones de seguridad	1056
Categorías de control	1059
Identificar	1060
Proteger	1061
Detect	1062
Respuesta	1062
Recuperar	1063
Visualización de los detalles de un control	1063
Visualización de detalles de un control	1064
Controles de filtrado y clasificación	1066
Parámetros de control	1067
Efecto de la modificación de los valores de parámetros de control	1068
Controles que admiten parámetros personalizados	1070
Revisión de los valores actuales de los parámetros de control	1070
Personalización de parámetros de control	1072
Reversión de los parámetros de control predeterminados	1077
Comprobación del estado de los cambios de los parámetros de control	1081
Visualización y administración de los resultados de control	1082
Filtrado y clasificación de resultados de control	1083
Ejemplos de resultados de control en Security Hub	1084
Integraciones de Security Hub	1106
Visualizar una lista de integraciones	1107
Habilitación del flujo de resultados desde una integración	1108
Deshabilitación del flujo de resultados desde una integración	1109
Visualizar resultados desde una integración	1110
Servicio de AWS integraciones	1111
Descripción general de las integraciones de AWS servicios con Security Hub	1111
AWS servicios que envían los resultados a Security Hub	1112

AWS servicios que reciben las conclusiones de Security Hub	1130
Integraciones de terceros	1132
Descripción general de integraciones de terceros con Security Hub	1133
Integraciones de terceros que envían resultados a Security Hub	1142
Integraciones de terceros que reciben resultados de Security Hub	1159
Integraciones de terceros que envían y reciben resultados de Security Hub	1165
Integraciones de productos personalizados	1167
Requisitos y recomendaciones para las integraciones de productos personalizados	1167
Actualización de los resultados de los productos personalizados	1168
Integraciones personalizadas de ejemplo	1169
Resultados	1170
BatchImportFindings para encontrar proveedores	1171
Requisitos previos para utilizar BatchImportFindings	1171
Determinación de si se debe crear o actualizar un hallazgo	1171
Restricciones para la actualización de resultados con BatchImportFindings	1172
Actualización de los hallazgos con FindingProviderFields	1172
BatchUpdateFindings para clientes	1174
Campos disponibles para BatchUpdateFindings	1175
Configurar el acceso a BatchUpdateFindings	1175
Revisión de los detalles y el historial de resultados	1178
Instrucciones para revisar los detalles y el historial de los resultados	1180
Filtrado de resultados	1183
Filtros predeterminados en las listas de búsqueda	1184
Instrucciones para añadir filtros	1184
Agrupación de hallazgos	1186
Configurar el estado del flujo de trabajo	1187
Configuración del estado de flujo de trabajo de los resultados	1188
Envío de hallazgos a una acción personalizada	1190
Formato de los hallazgos	1190
ASFF y consolidación	1271
Atributos de nivel superior necesarios del ASFF	1334
Atributos de nivel superior opcionales del ASFF	1346
Resources Objeto ASFF	1366
Informaciones	1492
Visualización de hallazgos y resultados del conocimiento	1493
Visualización y adopción de medidas sobre los resultados de la información	1493

Para visualizar y tomar medidas sobre los hallazgos en los resultados de la información (consola)	1495
Conocimientos administrados	1496
Información personalizada	1507
Creación de hallazgos personalizados	1508
Edición de hallazgos personalizados	1511
Eliminación de hallazgos personalizados	1513
Automatizaciones	1516
Reglas de automatización	1517
Definición de criterios de regla y acciones de regla	1517
Criterios de regla y acciones de regla disponibles	1518
Resultados que las reglas de automatización evalúan	1524
Cómo funciona el orden de las reglas	1525
Creación de reglas de automatización	1526
Visualización de las reglas de automatización	1530
Edición de reglas de automatización	1531
Edición del orden de las reglas	1533
Eliminar o desactivar las reglas de automatización	1534
Ejemplos de reglas de automatización	1536
Respuesta y corrección automatizadas	1543
Tipos de eventos de Security Hub en EventBridge	1544
EventBridge formatos de eventos	1546
Configurar una regla para los resultados de Security Hub	1549
Configuración y uso de acciones personalizadas	1556
Panel de control	1561
Widgets disponibles para el panel Resumen	1561
Widgets mostrados de forma predeterminada	1561
Widgets ocultos de forma predeterminada	1563
Filtrado del panel Resumen	1564
Creación y almacenamiento de conjuntos de filtros	1565
Actualización o eliminación de conjuntos de filtros	1566
Personalización del panel Resumen	1566
Creación de recursos con CloudFormation	1568
Security Hub y AWS CloudFormation plantillas	1568
Obtenga más información sobre AWS CloudFormation	1569
Suscripción a los anuncios de Security Hub	1570

Formato de SNS mensaje de Amazon	1576
Seguridad	1578
Protección de los datos	1579
Identity and Access Management	1580
Público	1580
Autenticación con identidades	1581
Administración de acceso mediante políticas	1585
Cómo funciona Security Hub con IAM	1587
Ejemplos de políticas basadas en identidades	1596
Roles vinculados a servicios	1602
AWS políticas gestionadas	1605
Resolución de problemas	1617
Validación de conformidad	1621
Resiliencia	1622
Seguridad de la infraestructura	1622
VPCpuntos finales ()AWS PrivateLink	1623
Consideraciones sobre los puntos VPC finales de Security Hub	1623
Creación de un VPC punto final de interfaz para Security Hub	1623
Creación de una VPC política de puntos finales para Security Hub	1624
Subredes compartidas	1625
Registrar API llamadas	1626
Información sobre Security Hub en CloudTrail	1626
Ejemplo: entradas del archivo de registros de Security Hub	1627
Etiquetado de recursos	1629
Conceptos básicos del etiquetado	1629
Uso de etiquetas en políticas de IAM	1631
Agregar etiquetas.	1632
Edición de etiquetas de recursos	1634
Revisión de las etiquetas	1636
Eliminación de etiquetas	1639
Cuotas	1641
Cuotas máximas	1641
Cuotas de tarifas	1641
Límites regionales de Security Hub	1642
Restricciones de agregación entre regiones	1642
Disponibilidad de las integraciones por región	1642

Integraciones que son compatibles en China (Pekín) y China (Ningxia)	1642
Integraciones compatibles en AWS GovCloud (Este de EE. UU.) y AWS GovCloud (Oeste de EE. UU.)	1643
Disponibilidad de los estándares por región	1645
Disponibilidad de los controles por región	1645
Límites regionales para los controles de Security Hub	1645
Este de EE. UU. (Norte de Virginia)	1647
Este de EE. UU. (Ohio)	1647
Oeste de EE. UU. (Norte de California)	1648
Oeste de EE. UU. (Oregón)	1650
África (Ciudad del Cabo)	1651
Asia-Pacífico (Hong Kong)	1654
Asia-Pacífico (Yakarta)	1656
Asia-Pacífico (Hyderabad)	1662
Asia-Pacífico (Malasia)	1670
Asia-Pacífico (Melbourne)	1684
Asia-Pacífico (Bombay)	1693
Asia-Pacífico (Osaka)	1694
Asia-Pacífico (Seúl)	1700
Asia-Pacífico (Singapur)	1702
Asia-Pacífico (Sídney)	1703
Asia-Pacífico (Tokio)	1704
Canadá (centro)	1705
China (Pekín)	1706
China (Ningxia)	1716
Europa (Fráncfort)	1725
Europa (Irlanda)	1726
Europa (Londres)	1727
Europa (Milán)	1728
Europa (París)	1732
Europa (España)	1733
Europa (Estocolmo)	1744
Europa (Zúrich)	1745
Israel (Tel Aviv)	1754
Medio Oriente (Baréin)	1763
Oriente Medio (UAE)	1766

América del Sur (São Paulo)	1773
AWS GovCloud (EEUU-Este)	1774
AWS GovCloud (EEUU-Oeste)	1786
Deshabilitación de Security Hub	1798
Registro de cambios de controles	1801
Historial de documentos	1869
.....	mcmlixiv

¿Qué es AWS Security Hub?

AWS Security Hub le proporciona una visión completa del estado de su seguridad en AWS y lo ayuda a evaluar su entorno de AWS en relación con los estándares y las prácticas recomendadas del sector de la seguridad.

Security Hub recopila datos de seguridad de todas las Cuentas de AWS, los Servicios de AWS y los productos compatibles de terceros y lo ayuda a analizar sus tendencias de seguridad y a identificar los problemas de seguridad de mayor prioridad.

Para ayudarle a gestionar el estado de seguridad de su organización, Security Hub admite varios estándares de seguridad. Estos incluyen el estándar de prácticas recomendadas de seguridad básica de AWS desarrollado por AWS, y los marcos de cumplimiento externos, como el Centro para la seguridad de Internet (Center for Internet Security, CIS), el estándar de seguridad de datos del sector de las tarjetas de pago de EE. UU. (Payment Card Industry Data Security Standard, PCI DSS) y el Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST). Cada estándar incluye varios controles de seguridad, cada uno de los cuales representa una práctica de seguridad recomendada. Security Hub ejecuta comprobaciones de los controles de seguridad y genera resultados de control para ayudarle a evaluar su cumplimiento de las mejores prácticas de seguridad.

Además de generar resultados de control, Security Hub también recibe datos de otros Servicios de AWS (como Amazon GuardDuty, Amazon 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 los resultados de Security Hub a otros Servicios de AWS y productos de terceros compatibles.

Security Hub ofrece características 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 puede aprovechar la integración con Amazon EventBridge para activar respuestas automáticas a resultados específicos.

Temas

- [Ventajas de Security Hub](#)
- [Acceso a Security Hub](#)
- [Servicios relacionados](#)

- [Prueba gratuita y precios de Security Hub](#)

Ventajas de Security Hub

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

Reducción del esfuerzo para recopilar y priorizar los resultados

Security Hub reduce el esfuerzo de recopilar y priorizar los resultados de seguridad en todas las cuentas de Servicios de AWS integrados y de productos de socios de AWS. Security Hub procesa los datos de los resultados empleando Formato de resultados de seguridad de AWS (ASFF), un formato estándar para resultados. Esto elimina la necesidad de administrar los resultados de numerosas fuentes en varios formatos. Security Hub también correlaciona los resultados de los proveedores para ayudarle a priorizar los más importantes.

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

Security Hub ejecuta automáticamente controles de seguridad continuos y de configuración en el nivel de la cuenta en función de las prácticas recomendadas de AWS y de los estándares del sector. Security Hub utiliza los resultados de estas comprobaciones para calcular puntuaciones de seguridad e identifica cuentas y recursos específicos que requieren atención.

Vista consolidada de los resultados en cuentas y proveedores

Security Hub consolida los resultados de seguridad de las cuentas y los productos de proveedores y muestra los resultados en la consola de Security Hub. También puede recuperar los resultados a través de la API de Security Hub, la AWS CLI y los SDK. 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 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

Security Hub está disponible en la mayoría de Regiones de AWS. Para obtener una lista de todas las regiones en las que Security Hub se encuentra actualmente disponible, consulte [Puntos de conexión y cuotas de AWS Security Hub](#) en la Referencia general de AWS. Para obtener información sobre cómo administrar Regiones de AWS para su Cuenta de AWS, consulte [Especificación de las Regiones de AWS que puede utilizar su cuenta](#) en la Guía de referencia de AWS Account Management.

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

Consola de Security Hub

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

API de Security Hub

La API de Security Hub le da acceso programático a su cuenta, datos y recursos de Security Hub. Con la API, puede enviar solicitudes HTTPS directamente a Security Hub. Para obtener más información sobre la API, consulte la [Referencia de la API de AWS Security Hub](#).

AWS CLI

La AWS CLI le permite ejecutar comandos en la línea de comandos de su sistema para llevar a cabo tareas 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 acerca de la instalación y el uso de la AWS CLI, consulte la [Guía del usuario de AWS Command Line Interface](#).

SDK de AWS

AWS ofrece SDK que constan de bibliotecas y código de muestra para diversos lenguajes de programación y plataformas; por ejemplo, Java, Go, Python, C++ y .NET. Los SDK ofrecen un acceso práctico mediante programación a Security Hub y a otros Servicios de AWS en el idioma que prefiera. También se encargan de tareas como firmar solicitudes criptográficamente, gestionar los errores y reintentar las solicitudes de forma automática. Para obtener información de instalación y uso de los SDK de AWS, consulte [Herramientas para crear en AWS](#).

⚠ Important

Security Hub solo detecta y consolida los resultados que se generan después de habilitar Security Hub. Sin embargo, no lo hace retroactivamente; es decir, no detecta ni consolida los resultados que se generaron antes de habilitar Security Hub.

Security Hub solo recibe y procesa los resultados de la misma región en la que habilitó Security Hub en su cuenta.

Para satisfacer totalmente los controles de seguridad del indicador de referencia CIS AWS Foundations, debe habilitar Security Hub en todas las regiones de AWS admitidas.

Servicios relacionados

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

Para consultar una lista de otros Servicios de AWS que envían o reciben resultados de Security Hub, consulte [Servicio de AWS integraciones con Security Hub](#).

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

Prueba gratuita y precios de Security Hub

Cuando habilite Security Hub por primera vez en una Cuenta de AWS, la cuenta se inscribirá automáticamente en una prueba gratuita de Security Hub de 30 días.

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

No se le cobrará por utilizar Security Hub hasta que finalice la versión de prueba gratuita.

Visualización de detalles de uso y costo estimado

Security Hub proporciona información de uso, incluido un costo estimado de 30 días por el uso de Security Hub. Los detalles de uso incluyen el tiempo restante de la prueba gratuita. La información de uso puede ayudarte a entender cuáles pueden ser los costos de su Security Hub una vez finalizada 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 de AWS Security Hub en <https://console.aws.amazon.com/securityhub/>.
2. En el panel de navegación, elija Uso en Configuración.

El costo mensual calculado se basa en el uso de Security Hub de su cuenta para resultados y controles de seguridad durante un periodo 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 por los resultados recibidos y los controles de seguridad, consulte los [precios de Security Hub](#).

Conceptos de Security Hub

En este tema se describen los conceptos y la terminología clave AWS de Security Hub para ayudarle a empezar a utilizar el servicio.

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.

Una cuenta puede invitar a otras cuentas a activar Security Hub y asociarse a esa cuenta en Security Hub. 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 de Security Hub para la organización. La cuenta de administrador de Security Hub puede habilitar otras cuentas de la organización como cuentas miembro.

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 [Administración de cuentas de administrador y de miembro en Security Hub](#).

Cuenta de administrador

Una cuenta de Security Hub a la que se le concede acceso para ver los resultados de las cuentas miembro 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. 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 de Security Hub. La cuenta de administrador de Security Hub puede habilitar cualquier cuenta de la organización como cuenta miembro y también puede invitar a otras cuentas a convertirse en cuentas 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 de varios 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.

Consulte [Agregación entre regiones](#).

Resultado archivado

Un resultado que tiene un `RecordState` establecido en `ARCHIVED`. Archivar un resultado indica que el proveedor del mismo cree que dicho resultado ya no es relevante. El estado del registro es independiente del estado del flujo de trabajo, que realiza el seguimiento del estado de una investigación sobre un resultado.

Los proveedores de búsqueda pueden utilizar el [BatchImportFindings](#) funcionamiento del Security Hub API para archivar los hallazgos que hayan creado. Security Hub archiva automáticamente los resultados de los controles si se deshabilita el control o se elimina el recurso asociado, según uno de los criterios siguientes.

- El resultado no se actualiza en un plazo de tres a cinco días (tenga en cuenta que se hará todo lo posible y no está garantizado).
- Se devuelve AWS Config la evaluación asociada `NOT_APPLICABLE`.

Por defecto, los resultados archivados se excluyen de las listas de resultados en la consola de Security Hub. Puede actualizar el filtro para incluir los resultados archivados.

El [GetFindings](#) funcionamiento del Security Hub API devuelve tanto los hallazgos activos como los archivados. Puede incluir un filtro para el estado del registro.

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

```
    "Value": "ARCHIVED"  
  }  
],
```

AWS Formato de búsqueda de seguridad () ASFF

Un formato estandarizado para el contenido de los resultados que Security Hub agrega o genera. El formato AWS Security Finding le permite usar Security Hub para ver y analizar los hallazgos generados por los servicios de AWS seguridad, las soluciones de terceros o el propio Security Hub 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 IDs y títulos específicos de un estándar. Actualmente, Security Hub solo admite controles estándar en las regiones de AWS GovCloud (US) Region y China. Los controles de seguridad son compatibles en todas las demás regiones.

Acción personalizada

Un mecanismo de Security Hub al que enviar los hallazgos seleccionados a EventBridge. Se crea una acción personalizada en Security Hub. 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 Organizations, la cuenta de administrador delegado de un servicio puede administrar el uso de un servicio para la organización.

En Security Hub, la cuenta de administrador de Security Hub también es la cuenta de administrador delegado de Security Hub. Cuando la cuenta de administración de la organización

designa por primera vez una cuenta de administrador de Security Hub, Security Hub llama a las Organizations 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 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 genera un resultado tras completar el control de seguridad de un control. Estos se denominan resultados de control. Los resultados también pueden provenir de integraciones de productos de terceros.

Para obtener más información sobre los resultados de Security Hub, consulte [Resultados](#).

Note

Los resultados se eliminan al cabo 90 días de la última actualización o 90 días después de que se crearan si no hay actualizaciones. Para almacenar los hallazgos durante más de 90 días, puede configurar una regla EventBridge que dirija los hallazgos a su bucket de Amazon S3.

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.

Consulte [Agregación entre regiones](#).

Ingesta de resultados

La importación de los resultados a Security Hub 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 ofrece varias informaciones administradas (predeterminadas) que no puede modificar. También puede crear información personalizada sobre Security Hub para realizar un seguimiento de los problemas de seguridad exclusivos de su AWS entorno y uso. Para obtener más información, consulte [Informaciones](#).

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.

Consulte [Agregación entre 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.
- La cuenta de administrador de Security Hub habilita la cuenta de la organización como cuenta 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

Una point-in-time evaluación específica de una regla con respecto a un único recurso que resulta en un PASSEDFAILED,WARNING, o NOT_AVAILABLE estado. La ejecución de un control de seguridad produce un resultado.

Cuenta de administrador de Security Hub

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

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

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

La cuenta de administrador de Security Hub puede habilitar cualquier cuenta de la organización como cuenta miembro. La cuenta de administrador de Security Hub también puede invitar a otras cuentas a convertirse en cuentas miembro.

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. Para obtener más información sobre los estándares de seguridad en Security Hub, consulte [Descripción de los estándares de seguridad en Security Hub](#).

Gravedad

La gravedad asignada a un control 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 asigna Security Hub la gravedad a un control, consulte [Nivel de gravedad de los hallazgos de control](#).

Estado del flujo de trabajo

El estado de una investigación sobre un resultado. Se realiza un seguimiento 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 de Security Hub proporciona una opción para establecer el estado del flujo de trabajo de los resultados. Los clientes (o las herramientas de venta de entradas SIEM, gestión de incidentes o SOAR herramientas que trabajan en nombre de un cliente para actualizar los resultados obtenidos al buscar proveedores) también pueden utilizar [BatchUpdateFindings](#) para actualizar el estado del flujo de trabajo.

Habilitación de Security Hub

Hay dos formas de habilitar AWS 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 Security Hub manualmente.

Verificación de los permisos necesarios

Después de registrarse en Amazon Web Services (AWS), debe habilitar Security Hub para utilizar sus capacidades y características. Para habilitar Security Hub, primero debe configurar los permisos que le permitan acceder a la consola y API las operaciones del Security Hub. Para ello, usted o su AWS administrador pueden utilizar AWS Identity and Access Management (IAM) para adjuntar la política AWS gestionada llamada `AWSecurityHubFullAccess` a su IAM identidad.

Para habilitar y administrar Security Hub 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 AWS Security Hub](#).

Habilitación de la integración de Security Hub con Organizations

Para empezar a usar Security Hub con AWS Organizations, la cuenta AWS Organizations de administración de la organización designa una cuenta como la cuenta de administrador delegada del Security Hub para la organización. 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 console

Para designar el administrador de Security Hub delegado al incorporarse

1. Abra la consola AWS de Security Hub en <https://console.aws.amazon.com/securityhub/>.
2. Seleccione Ir a Security Hub. 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 API

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

AWS CLI

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

Configuración centralizada

Al integrar Security Hub y Organizations, tiene la opción de usar una función llamada [configuración central](#) para configurar y administrar Security Hub 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 en todas las cuentas OUs, y Regiones de AWS. El administrador delegado configura Security Hub al crear políticas de configuración. Dentro de una política de configuración, puede especificar la siguiente configuración:

- Si se habilita o deshabilita Security Hub
- 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 usa la configuración centralizada, debe configurar Security Hub, en gran medida, por separado en cada cuenta y región. Esto se denomina [configuración local](#). En la configuración local, el administrador delegado puede habilitar automáticamente Security Hub 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.

Habilitación de manual de Security Hub

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

Al habilitar Security Hub manualmente, designa una cuenta de administrador de este servicio 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 estos pasos para habilitar Security Hub. Al habilitar Security Hub desde la consola, también tiene la opción de habilitar los estándares de seguridad admitidos.

Security Hub console

1. Abra la consola AWS de Security Hub en <https://console.aws.amazon.com/securityhub/>.

2. Al abrir la consola de Security Hub por primera vez, seleccione Vaya a Security Hub.
3. En la página de bienvenida, la sección Estándares de seguridad enumera los estándares de seguridad que admite Security Hub.

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](#).

4. Seleccione Habilitar Security Hub.

Security Hub API

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

- AWS Mejores prácticas de seguridad fundamentales
- Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0

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
- Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0

```
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, se recomienda utilizar la configuración centralizada para habilitar y configurar Security Hub en varias cuentas y regiones.

El [script de activación de múltiples cuentas de Security Hub GitHub le permite habilitar 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 AWS Config recursos de todos los recursos, incluidos los recursos 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 el correspondiente script que permite deshabilitar Security Hub en todas las cuentas y regiones.

Próximos pasos: gestión de la postura e integraciones

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

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

Activación y configuración AWS Config de Security Hub

AWS Security Hub usa AWS Config reglas para ejecutar controles de seguridad y generar resultados para la mayoría de los controles. AWS Config proporciona una vista detallada de la configuración de AWS los 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.

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

Para recibir los resultados de control en Security Hub, 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 activar AWS Config Security Hub y cómo activar el registro de recursos.

Consideraciones antes de habilitar y configurar AWS Config

Para recibir los resultados de control en Security Hub, su cuenta debe estar AWS Config habilitada en todos los Región de AWS lugares donde Security Hub esté habilitado. Si usa Security Hub para un entorno de varias cuentas, AWS Config debe estar habilitado en cada región en la cuenta de administrador y en todas las cuentas de los miembros.

Le recomendamos encarecidamente que active el registro de recursos AWS Config antes de activar los estándares y controles 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 a la grabadora de configuración. Además, asegúrese de que no haya ninguna IAM política o política administrada AWS Organizations que AWS Config impida tener permiso para registrar sus recursos. Las comprobaciones de control de Security Hub evalúan directamente la configuración de un recurso y no tienen en cuenta las políticas de Organizations. Para obtener más información sobre el AWS Config registro, consulte [la Lista de reglas AWS Config administradas: consideraciones](#) en la Guía para AWS Config desarrolladores.

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

- El día en que se active el estándar
- Al día después de activar el estándar
- 3 días después de habilitar el estándar
- 7 días después de habilitar el estándar (y posteriormente cada 7 días)

Si utilizas la configuración central, Security Hub también intenta crear las reglas AWS Config vinculadas al servicio cada vez que asocias 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 AWS Config habilitarla, 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 a Security Hub detectar cambios en las configuraciones de los recursos.

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

Warning

Si no configura correctamente la AWS Config grabación de los controles de Security Hub, se pueden producir resultados de control imprecisos, especialmente en los siguientes casos:

- Nunca registró el recurso para un control determinado, deshabilitó el registro de un recurso antes de crear ese tipo de recurso o asignó un IAM rol al registrador de configuración que no proporcionara permisos para grabar el recurso. En estos casos, recibirá una confirmación PASSED sobre el control en cuestión, aunque es posible que haya creado recursos dentro del ámbito del control después de deshabilitar el registro. Este PASSED resultado es un resultado predeterminado que en realidad no evalúa el estado de configuración del recurso.
- Se deshabilita el registro de un recurso evaluado por un control en particular. En este caso, Security Hub conserva las conclusiones de control que se generaron antes de deshabilitar

la grabación, aunque el control no evalúe los recursos nuevos o actualizados. Es posible que estos resultados 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 lugar Región de AWS en el que se está ejecutando. Para recibir todos los resultados de control de Security Hub, también debe configurarlo AWS Config para que registre 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 periodo de 24 horas si se producen cambios en el estado de dichos recursos. Si no hay cambios, no se entrega ningún dato. Esto puede retrasar la generación de las conclusiones 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 [AWS los recursos de grabación en la Guía para AWS Config](#) desarrolladores.

Formas de habilitar y configurar AWS Config

Puede habilitar AWS Config y activar el registro de recursos de una 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: si desea habilitarlo AWS Config para un gran número de cuentas, le recomendamos que utilice la AWS CloudFormation plantilla denominada Enable AWS Config. Para acceder a esta plantilla, consulte [las plantillas AWS CloudFormation StackSets de muestra](#) en la Guía del AWS CloudFormation usuario.

De forma predeterminada, esta plantilla excluye el registro de recursos IAM globales. Asegúrese de activar la grabación para los recursos IAM globales de una sola región a fin de ahorrar costes de grabación. Si tiene habilitada la agregación entre regiones, esta debería ser la [región de origen de su Security Hub](#). De lo contrario, puede ser cualquiera en el Región de AWS que esté disponible Security Hub y que permita el registro de recursos IAM globales. Recomendamos ejecutar uno StackSet para registrar todos los recursos, incluidos los recursos IAM globales, de la región de origen o de otra región seleccionada. A continuación, ejecuta un segundo StackSet para registrar todos los recursos excepto los recursos IAM globales de otras regiones.

- Secuencia de comandos de Github: Security Hub ofrece una [GitHub secuencia de comandos](#) que habilita Security Hub y AWS Config para múltiples cuentas en todas las regiones. Este script es útil si no te has integrado con Organizations o si tienes algunas cuentas de miembros que no forman parte de una organización.

Para obtener más información, consulte [Optimizar AWS ConfigAWS Security Hub para gestionar de forma eficaz su estrategia de seguridad en la nube](#).

Control de configuración 1

La [configuración de control Security Hub 1](#) genera FAILED resultados en su cuenta si AWS Config está deshabilitada o si no tiene activado el registro de recursos para los controles habilitados. Si es el administrador delegado de Security Hub de una organización, el AWS Config registro debe estar correctamente configurado en su cuenta y en las cuentas de los miembros. Si utiliza la agregación entre regiones, la AWS Config grabación debe estar configurada correctamente en la región de origen y en todas las regiones vinculadas (no es necesario que los recursos globales se registren en las regiones vinculadas).

Para recibir información sobre Config.1, active el registro de recursos para todos los recursos que correspondan a los controles de Security Hub habilitados y deshabilite los controles que no sean necesarios en su organización. PASSED Esto ayuda a garantizar que no haya brechas de configuración en sus comprobaciones de control de seguridad y que reciba información precisa sobre recursos mal configurados.

Generación de reglas vinculadas a servicios

Para cada control que utilice una regla AWS Config vinculada a un servicio, Security Hub crea instancias de la regla requerida en su AWS entorno.

Estas reglas vinculadas a servicios son específicas de Security Hub. Security Hub 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 gestionadavpc-flow-logs-enabled`, el nombre de la regla vinculada al servicio sería algo parecido a: `securityhub-vpc-flow-logs-enabled-12345`

Hay límites en la cantidad de reglas AWS Config administradas que se pueden usar para evaluar los controles. AWS Config Las reglas personalizadas que crea Security Hub no cuentan para ese límite. Puedes habilitar un estándar de seguridad incluso si ya has alcanzado el AWS Config límite de reglas administradas en tu cuenta. Para obtener más información sobre los límites de las AWS Config reglas, consulta [los límites de servicio AWS Config en la Guía para AWS Config desarrolladores](#).

Consideraciones sobre costos

Security Hub puede afectar a los costes AWS Config de la grabadora de configuración al actualizar el elemento `AWS::Config::ResourceCompliance` de configuración. Las actualizaciones se pueden producir cada vez que un control de Security Hub asociado a una AWS Config regla cambia de estado de conformidad, se habilita o deshabilita, o se actualiza sus parámetros. Si usa la grabadora de AWS Config configuración solo para Security Hub 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 registrar los controles de seguridad de `AWS::Config::ResourceCompliance` para que funcione en Security Hub.

Para obtener más información acerca de los costos asociados al registro de recursos, consulte [Precios de AWS Security Hub](#) y [Precios de AWS Config](#).

Descripción de la configuración local en Security Hub

La configuración local es la forma predeterminada en que se configura una organización de AWS en Security Hub. 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 delegado de Security Hub tiene control limitado sobre los ajustes de configuración. Los únicos ajustes que el administrador delegado puede aplicar son habilitar automáticamente Security Hub 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 las Prácticas

recomendadas de seguridad básica de AWS v1.0.0 (FSBP) e Indicador de referencia de AWS v1.2.0 de Center for Internet Security (CIS). 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 Security Hub y los estándares predeterminados en las nuevas cuentas de la organización en una sola región, debe configurar otros ajustes 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 [Comprensión de la configuración centralizada en Security Hub](#).

Comprensión de la configuración centralizada en Security Hub

La configuración centralizada es una característica de Security Hub que le ayuda a configurar y administrar el servicio en múltiples Cuentas de AWS y Regiones de AWS. Para usar la configuración centralizada, antes debe integrar Security Hub y AWS Organizations. Para integrar los servicios, puede crear una organización y designar una cuenta de administrador delegado de Security Hub para la organización.

Desde la cuenta de administrador delegado de Security Hub, puede especificar cómo se configuran el servicio Security Hub, los estándares de seguridad y controles de seguridad en las cuentas y las unidades organizativas (OU) de su organización en todas las regiones. Puede configurar estos ajustes en tan solo unos pasos desde una región principal, denominada región de origen.

Al utilizar la configuración centralizada, el administrador delegado puede elegir qué cuentas y unidades organizativas desea 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 y unidades organizativas de su organización como administradas de forma centralizada, todas autoadministradas o como una combinación de ambas.

Para configurar las cuentas administradas de forma centralizada, el administrador delegado utiliza las políticas de configuración de Security Hub. Las políticas de configuración permiten al administrador delegado especificar si Security Hub está habilitado o deshabilitado, y qué normas y controles están habilitados o deshabilitados. También pueden utilizarse 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 única política de configuración para toda la organización, o crear varias políticas de configuración para configurar ajustes variables en diferentes cuentas y unidades organizativas.

Tip

Si no usa la configuración centralizada, debe configurar Security Hub, en gran medida, por separado en cada cuenta y región. Esto se denomina configuración local. En la configuración local, el administrador delegado puede habilitar automáticamente Security Hub 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:

Simplificación de la configuración del servicio y las capacidades de Security Hub

Cuando utiliza la configuración centralizada, Security Hub le guía a través del proceso de configuración de las prácticas recomendadas de seguridad para su organización. También implementa automáticamente las políticas de configuración resultantes en cuentas y unidades organizativas específicas. Si ya tiene configuraciones existentes en Security Hub, como habilitar automáticamente nuevos controles de seguridad, puede utilizarlas como punto de partida para las políticas de configuración. Además, la página Configuración de la consola de Security Hub muestra un resumen en tiempo real de las políticas de configuración y cuentas y unidades organizativas que utiliza cada política.

Configuración en todas las cuentas y regiones

Puede utilizar la configuración centralizada para configurar Security Hub 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.

Compatibilidad con diferentes configuraciones en diferentes cuentas y unidades organizativas

Con la configuración centralizada, puede elegir si desea configurar las cuentas y unidades organizativas de su organización de diferentes 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 centralizada es más beneficiosa para los entornos de AWS que incluyen varias cuentas de Security Hub. Está diseñada para ayudarle a administrar Security Hub en varias cuentas.

Puede usar la configuración centralizada para configurar el servicio 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](#). Para más información sobre los controles de seguridad, consulte [Descripción de los controles de seguridad en Security Hub](#).

Términos y conceptos de la configuración centralizada

Comprender los siguientes términos y conceptos clave puede ayudarle a utilizar la configuración centralizada de Security Hub.

Configuración centralizada

Una característica de Security Hub que ayuda a la cuenta de administrador delegado de Security Hub de una organización a configurar el servicio 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 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 centralizada, debe integrar Security Hub y AWS Organizations.

Región de origen

La Región de AWS desde la cual el administrador delegado configura de manera centralizada Security Hub mediante la creación y la 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 sirve como la región de agregación de Security Hub que recibe resultados, información y otros datos de las regiones vinculadas.

Las regiones que AWS introdujo después del 20 de marzo de 2019 son regiones optativas. 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

Una Región de AWS que se puede 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 introdujo después del 20 de marzo de 2019 son regiones optativas. 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, consulte [Specify which Regions de AWS your account can use](#) en la Guía de referencia de administración de cuentas de AWS.

Destino

Una Cuenta de AWS, una unidad organizativa (OU) o la raíz de la organización.

Política de configuración de Security Hub

Un conjunto de ajustes de Security Hub que el administrador delegado puede configurar para los destinos administrados de forma centralizada. Esto incluye:

- Si se habilita o deshabilita Security Hub.
- Si se habilitan uno o más [estándares de seguridad](#).
- Qué [controles de seguridad](#) se habilitan en todos los estándares habilitados. Para hacerlo, el administrador delegado puede proporcionar una lista de controles específicos que deben estar habilitados, y Security Hub deshabilitará todos los demás controles (incluidos los controles nuevos cuando se lanzan). Como alternativa, el administrador delegado puede proporcionar una lista de controles específicos que deberían estar deshabilitados y Security Hub habilitará todos los demás controles, lo que incluye los controles nuevos cuando se lanzan.
- 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 de Security Hub, el administrador delegado puede elegir la política de configuración recomendada por Security Hub o crear políticas de configuración personalizadas. Con la API de Security Hub y la 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 para Security Hub, se habilitan las Prácticas recomendadas de seguridad básica de AWS (FSBP) y todos los controles existentes y nuevos de

FSBP. Los controles que aceptan parámetros utilizan los valores predeterminados. La política de configuración recomendada se aplica a toda la organización.

Para aplicar diferentes configuraciones a la organización o aplicar diferentes políticas de configuración a diferentes cuentas y unidades organizativas, cree una política de configuración personalizada.

Configuración local

El tipo de configuración predeterminado para una organización, después de integrar Security Hub y AWS Organizations. Con la configuración local, el administrador delegado puede habilitar automáticamente Security Hub, 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 con AWS Organizations o si 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.

API de configuración centralizada

Operaciones de Security Hub que solo el administrador delegado de Security Hub puede usar en la región de origen para administrar políticas de configuración para cuentas administradas centralmente. Las operaciones incluyen:

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`

- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

API específicas de la cuenta

Operaciones de Security Hub que se pueden utilizar para habilitar o deshabilitar Security Hub, los estándares y los controles cuenta por cuenta. 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 su cuenta, el propietario de una cuenta administrada de forma centralizada puede utilizar cualquiera de las operaciones `Get` o `Describe` de la API 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 y en Security Hub, un contenedor para un grupo de Cuentas de AWS. Una unidad organizativa (OU) también puede contener otras unidades organizativas, lo que le permite crear una jerarquía que se asemeja a un árbol invertido, con una unidad organizativa principal en la parte superior y ramas de unidades organizativas que descienden y terminan en cuentas que son las hojas del árbol. Una unidad organizativa puede tener una unidad principal y cada cuenta de la organización puede ser miembro de exactamente una unidad organizativa.

Puede administrar las unidades organizativas 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 o unidades organizativas específicas, o a la cuenta raíz para abarcar todas las cuentas y unidades organizativas 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 destino que administra su propia configuración de Security Hub. Un destino autoadministrado utiliza operaciones específicas de la cuenta para configurar 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, a las unidades organizativas o a la cuenta 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 cuenta raíz, la política de configuración afecta a todas las cuentas y unidades organizativas de la organización que no utilicen una configuración diferente mediante la aplicación o la herencia de la cuenta principal más cercana.

El administrador delegado también puede aplicar una configuración autoadministrada a cuentas específicas, unidades organizativas o la raíz.

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 y Security Hub, el nodo principal de nivel superior de una organización. Si el administrador delegado aplica una política de configuración a la cuenta raíz, la política se asocia a todas las cuentas y unidades organizativas de la organización, a menos que utilicen una política diferente, por aplicación o herencia, o se designen como autoadministradas. Si el administrador designa la raíz como autoadministrada, todas las cuentas y unidades organizativas de la organización se autoadministran, a menos que utilicen una política de configuración por aplicación o herencia. 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.

Habilitar la configuración centralizada en Security Hub

La cuenta de administrador delegado de AWS Security Hub puede utilizar la configuración centralizada en Security Hub, sus estándares y controles para varias cuentas y unidades organizativas (OU) en varias Regiones de AWS.

Para obtener información general sobre las ventajas de la configuración centralizada y su funcionamiento, consulte [Comprensión de la configuración centralizada en Security Hub](#).

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 centralizada, debe integrar Security Hub con AWS Organizations y designar una región de origen. Si utiliza la consola de Security Hub, estos requisitos previos se incluyen en el flujo de trabajo opcional para dicha configuración.

Integración con Organizations

Debe integrar Security Hub y Organizations para utilizar la configuración centralizada.

Para integrar estos servicios, comience por crear una organización en Organizations. Desde su cuenta de administración de Organizations, designe una cuenta como administrador delegado de Security Hub. Para obtener instrucciones, consulte [Integración de Security Hub 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 utiliza la configuración centralizada, no puede utilizar la consola o las API de Security Hub para cambiar o eliminar la cuenta de administrador delegado. Si la cuenta de administración de Organizations utiliza las API de AWS Organizations para cambiar o eliminar al administrador delegado de Security Hub, este último detiene automáticamente la configuración centralizada. 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 que AWS haya designado como región optativa. 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 centralizada, Security Hub deshabilita automáticamente los controles que implican 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 Security Hub que recibe resultados, 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 resultados es un recurso 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 console

Para habilitar la configuración centralizada (consola)

1. Abra la consola de AWS Security Hub 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 está incorporando a Security Hub, seleccione Vaya a Security Hub.

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 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 a la cuenta que llama como administrador delegado de Security Hub en todas las regiones vinculadas.
 - Habilita Security Hub en la cuenta de administrador delegado en todas las regiones vinculadas.
 - Designa a la cuenta que llama como administrador delegado de Security Hub para las cuentas nuevas y existentes que utilizan dicho servicio 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 que llama se configura como administrador delegado de las cuentas de la organización existentes solo si ya tienen habilitado 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 ni en las vinculadas cuando se utiliza la configuración centralizada, pero puede habilitar Security Hub automáticamente 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 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 a la cuenta que llama como administrador delegado de Security Hub en todas las regiones vinculadas.

- Habilita Security Hub en la cuenta de administrador delegado en todas las regiones vinculadas.
 - Designa a la cuenta que llama como administrador delegado de Security Hub para las cuentas nuevas y existentes que utilizan dicho servicio 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 que llama se configura como administrador delegado de las cuentas de la organización existentes solo si ya tienen habilitado 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 ni en las vinculadas cuando se utiliza la configuración centralizada, pero puede habilitar Security Hub automáticamente 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 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 AWS Security Hub administrador delegado 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 destino determina cómo se puede especificar la configuración de Security Hub.

Para obtener información general sobre las ventajas de la configuración centralizada y su funcionamiento, consulte [Comprensión de la configuración centralizada en Security Hub](#).

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 raíz 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 delegado de Security Hub 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 autogestionan al iniciar la configuración central a través del Security HubAPI. 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 administrada centralmente podría asociarse inicialmente a una política que habilitara Security Hub, habilitara AWS Foundational Security Best Practices v1.0.0 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 del Security Hub API en cada región para configurar sus ajustes:

- `EnableSecurityHub` y `DisableSecurityHub` para habilitar o deshabilitar el servicio Security Hub (si una cuenta autoadministrada tiene un administrador delegado de Security Hub, el administrador debe [desasociar la cuenta](#) antes de que el propietario de la cuenta pueda deshabilitar Security Hub).
- `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 API acciones de Security Hub, consulte la [AWS Security Hub APIReferencia](#).

Las cuentas autogestionadas también pueden usar la consola de Security Hub o AWS CLI configurar sus ajustes en cada región.

Las cuentas autogestionadas no pueden invocar ninguna política de configuración o asociación de políticas 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 una unidad organizativa como administrada de forma centralizada o autoadministrada en AWS Security Hub.

Security Hub console

Elección del tipo de administración de una cuenta o unidad organizativa

1. Abra la AWS Security Hub consola en. <https://console.aws.amazon.com/securityhub/>
Inicie sesión con las credenciales de la cuenta de administrador delegado de Security Hub en la región de origen.
2. Elija Configuración.
3. En la pestaña Organización, seleccione la cuenta o la unidad organizativa de destino. Elija 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 Next (Siguiente). Revise los cambios y seleccione Guardar.

Security Hub API

Elección del tipo de administración de una cuenta o unidad organizativa

1. Invoca el [StartConfigurationPolicyAssociation](#) API desde la cuenta de administrador delegado 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. Proporcione el nombre del 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 la OU.

3. En el Target campo, indique 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 API solicitud para designar una cuenta autogestionada:

```
{
  "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
  "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Elección del tipo de administración de una cuenta o unidad organizativa

1. Ejecute la [start-configuration-policy-association](#) comando desde la cuenta de administrador delegado 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. Proporcione el nombre del 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 la unidad organizativa.
3. En el `target` campo, indique 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"}'
```

Funcionamiento de las políticas de configuración en Security Hub

El AWS Security Hub administrador delegado puede crear políticas de configuración para configurar 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 (OUs) o a la raíz específicas. 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 [Comprensión de la configuración centralizada en Security Hub](#).

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, tenga en cuenta los siguientes detalles.

- Las políticas de configuración deben estar asociadas para que surtan efecto: después de crear una política de configuración, puedes 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 deshabilita automáticamente los controles que implican 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 conocen como regiones con 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 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). ARN utiliza el siguiente formato: `arn:partition:securityhub:region:delegated administrator account ID:configuration-policy/configuration policy UUID`. Una configuración autogestionada 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:

- Habilite o deshabilite Security Hub.
- Habilite uno o más [estándares de seguridad](#).
- Indique qué [controles de seguridad](#) están habilitados en todos los estándares habilitados. Para ello, proporcione una lista de controles específicos que deberían estar habilitados y Security Hub deshabilitará todos los demás controles, lo que incluye los controles nuevos cuando se lanzan. De forma alternativa, proporcione una lista de controles específicos que deberían estar deshabilitados

y Security Hub habilitará todos los demás controles, lo que incluye los controles nuevos cuando se lanzan.

- 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 genere hallazgos de control. Para obtener más información, consulte [Consideraciones antes de habilitar y configurar AWS Config](#).

Si usa la configuración centralizada, Security Hub deshabilita automáticamente los controles que implican 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 los resultados 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 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 de Security Hub, tiene la opción de elegir la política recomendada por Security Hub.

La política recomendada habilita Security Hub, el estándar AWS Foundational Security Best Practices (FSBP), y todos los FSBP controles nuevos y existentes. Los controles que aceptan parámetros utilizan los valores predeterminados. La política recomendada se aplica a las cuentas root (todas las cuentas OUs, tanto las nuevas como las existentes). 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 FSBP controles específicos. 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 FSBP habilite Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 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 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 aparece la opción de crear la política de configuración recomendada en la consola 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

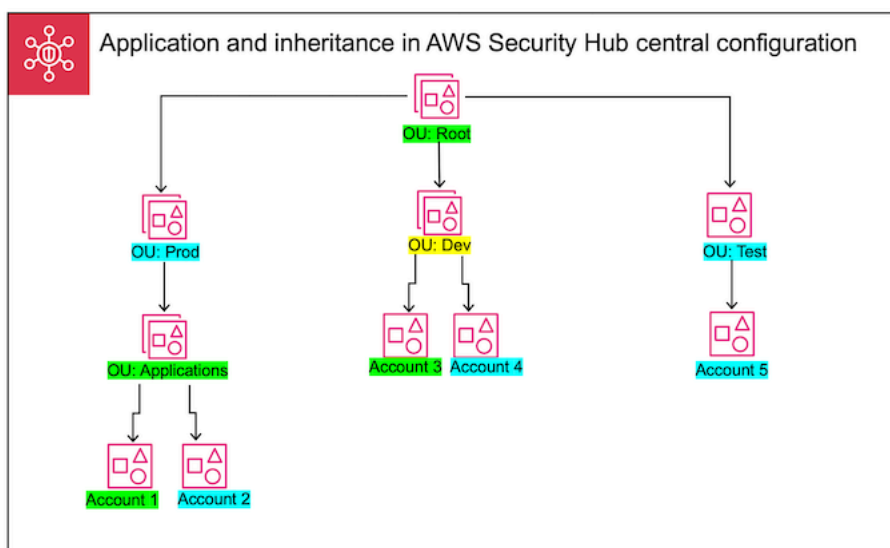
La aplicación tiene prioridad sobre la herencia. En otras palabras, la herencia no anula una política de configuración o una designación autoadministrada que el administrador delegado haya aplicado directamente a una cuenta o unidad organizativa.

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 activación, los estándares y los controles 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 AWS Security Hub administrador delegado puede crear políticas de configuración que especifiquen cómo se configuran Security Hub, los estándares y los controles en cuentas y unidades organizativas específicas (OUs). Una política de configuración solo entra en vigor después de que el administrador delegado la asocie a al menos 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 [Funcionamiento de las políticas de configuración en Security Hub](#).

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 de Security Hub, puede asociar una configuración a varias cuentas o OUs al mismo tiempo. Al utilizar el Security Hub API o AWS CLI, puede asociar una configuración a una sola cuenta o unidad organizativa en cada solicitud.

Note

Si usa la configuración centralizada, Security Hub deshabilita automáticamente los controles que implican 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 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 console

Creación y asociación de políticas de configuración

1. Abra la AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>.

Inicie sesión con las credenciales de la cuenta de administrador delegado de Security Hub 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 de Security Hub AWS recomendada en toda mi organización para usar nuestra política recomendada. La política recomendada habilita Security Hub en todas las cuentas de la organización, habilita el estándar AWS Foundational Security Best Practices (FSBP) y habilita todos los FSBP controles 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 Security Hub, qué estándares desea habilitar y qué controles desea 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 usuarios raíz) 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 Next (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 API

Creación y asociación de políticas de configuración

1. Invoque el [CreateConfigurationPolicy](#) API desde la cuenta de administrador delegado 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. En el campo ServiceEnabled, especifique si desea que Security Hub esté habilitado o deshabilitado en esta política de configuración.
4. En el campo EnabledStandardIdentifiers, especifique qué estándares de Security Hub desea 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 que especifique Security Hub. Solo algunos controles admiten valores de parámetros personalizados. Para obtener más información, consulte [Descripción de los parámetros de control en Security Hub](#).

7. Para aplicar su política de configuración a las cuentas oOUs, invoque la [StartConfigurationPolicyAssociationAPI](#) desde la cuenta de administrador delegado de Security Hub en la región de origen.
8. Para el `ConfigurationPolicyIdentifier` campo, proporciona el nombre del recurso de Amazon (ARN) o el identificador único universal (UUID) de la política. Los ARN y UUID son devueltos por `CreateConfigurationPolicyAPI`. 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 puedes proporcionar un objetivo en cada API solicitud. 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 API solicitud 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": {
```


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 que especifique Security Hub. Solo algunos controles admiten valores de parámetros personalizados. Para obtener más información, consulte [Descripción de los parámetros de control en Security Hub](#).
7. Para aplicar la política de configuración a las cuentas oOUs, ejecute el [start-configuration-policy-association](#) comando desde la cuenta de administrador delegado de Security Hub en la región de origen.
8. Para el `configuration-policy-identifier` campo, proporciona el nombre del recurso de Amazon (ARN) o el ID de la política de configuración. El `create-configuration-policy` comando devuelve este dato ARN y el identificador.
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"}'
```

`StartConfigurationPolicyAssociationAPI` 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 la política de configuración

El AWS Security Hub administrador delegado 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 [Comprensión de la configuración centralizada en Security Hub](#).

Elija su método preferido y siga estos pasos para ver las políticas de configuración.

Security Hub console

Para ver políticas de configuración (consola)

1. Abra la AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>.

Inicie sesión con las credenciales de la cuenta de administrador delegado de Security Hub 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 OUs que está asociada.

Security Hub API

Para ver una lista resumida de todas sus políticas de configuración, utilice la [ListConfigurationPolicies](#)funcionamiento del Security HubAPI. Si usa el AWS CLI, ejecute el [list-configuration-policies](#)comando. La cuenta de administrador delegado de Security Hub debe invocar la operación en la región de origen.

```
$ aws securityhub list-configuration-policies \  
--max-items 5 \  
--starting-token U2Fs dGVkX19nUI2zoh+Pou9YyutLYJHWpn9xnG4hqS0hvw3o2JqjI23QDxdf
```

Para ver los detalles de una política de configuración específica, utilice el [GetConfigurationPolicy](#)operación. Si usa la AWS CLI, ejecute la [get-configuration-policy](#). La cuenta de administrador delegado debe invocar la operación en la región de origen. Proporcione el nombre del 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-EXAMPLE11111"
```

Para ver una lista resumida de todas sus políticas de configuración y sus asociaciones de cuentas, utilice el [ListConfigurationPolicyAssociations](#)operación. Si usa la AWS CLI, ejecute la [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 el [GetConfigurationPolicyAssociation](#)operación. Si usa la AWS CLI, ejecute la [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 API operaciones de configuración central 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 Security Hub, habilite AWS Foundational Security Best Practices v1.0.0 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 secundaria o una unidad organizativa cambia (por ejemplo, cuando se agrega o elimina una región vinculada) después de asociar por primera vez la matriz a una configuración, el cambio no actualiza el estado de asociación de la cuenta principal a menos que se `StartConfigurationPolicyAssociation` API vuelva a invocar.
- 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 matriz, a menos que se vuelva a invocar `StartConfigurationPolicyAssociationAPI`.

Si agrega una nueva región vinculada, Security Hub replica las asociaciones existentes que se encuentran en un estado `PENDING`, `SUCCESS` o `FAILED` en la nueva región.

Solución de problemas de la asociación

En AWS Security Hub, la asociación de una política de configuración puede fallar por los siguientes motivos habituales.

- La cuenta de administración de Organizations no es miembro: si desea asociar una política de configuración a la cuenta de administración de Organizations, esa cuenta ya debe estar AWS Security Hub habilitada. 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 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 AWS Security Hub administrador delegado 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 [Comprensión de la configuración centralizada en Security Hub](#).

El administrador delegado puede actualizar los siguientes ajustes de la política:

- Habilite o deshabilite Security Hub.
- Habilite uno o más [estándares de seguridad](#).
- Indique qué [controles de seguridad](#) están habilitados en todos los estándares habilitados. Para ello, proporcione una lista de controles específicos que deberían estar habilitados y Security Hub deshabilitará todos los demás controles, lo que incluye los controles nuevos cuando se lanzan. De forma alternativa, proporcione una lista de controles específicos que deberían estar deshabilitados y Security Hub habilitará todos los demás controles, lo que incluye los controles nuevos cuando se lanzan.
- 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 centralizada, Security Hub deshabilita automáticamente los controles que incluyen 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 los resultados 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 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](#).

[Controles que utilizan recursos globales](#).

Console

Actualización de las políticas de configuración

1. Abra la AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>.


Inicie sesión con las credenciales de la cuenta de administrador delegado de Security Hub 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 Next (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 de Security Hub en la región de origen.
2. Proporcione el nombre del 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 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 de Security Hub en la región de origen.
5. Para el ConfigurationPolicyIdentifier campo, proporcione 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 el UpdateConfigurationPolicy API, Security Hub sustituye por una lista completa los SecurityControlCustomParameters campos EnabledStandardIdentifiersEnabledSecurityControlIdentifiers, DisabledSecurityControlCustomParametersEnabledStandardIdentifiers, DisabledSecurityControlCustomParametersEnabledSecurityControlIdentifiers y. Cada vez que lo invoque 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 API solicitud 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 parámetros de una política de configuración, ejecute el [update-configuration-policy](#) comando desde la cuenta de administrador delegado de Security Hub en la región de origen.
2. Proporcione el nombre del 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 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 de Security Hub en la región de origen.
5. Para el `configuration-policy-identifier` campo, proporcione 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 comando `update-configuration-policy`, Security Hub sustituye por completo la lista de los campos `EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiers`, `DisabledSecurityControlIdentifiers` 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}}}]}}}'
```

StartConfigurationPolicyAssociationAPI 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

Después de crear una política de configuración, el administrador delegado de AWS Security Hub puede eliminarla. Como alternativa, el administrador delegado puede retener la política, pero desasociarla de cuentas o de unidades organizativas (OU) específicas, 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 [Comprensión de la configuración centralizada en Security Hub](#).

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, las unidades organizativas y la raíz de la organización ya no pueden utilizar la política de configuración. 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.

Antes de eliminar una política de configuración, debe desasociarla de cualquier cuenta, unidad organizativa o raíz a la que se aplique en la actualidad.

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 de AWS Security Hub en <https://console.aws.amazon.com/securityhub/>.

Inicie sesión con las credenciales de la cuenta de administrador delegado de Security Hub 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 unidad organizativa, se le solicitará que desasocie antes 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 API [DeleteConfigurationPolicy](#) desde la cuenta de administrador delegado 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 error `ConflictException`, la política de configuración seguirá aplicándose a las cuentas o unidades organizativas de su organización. Para resolver el error, desasocie la política de configuración de estas cuentas o unidades organizativas 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 comando [delete-configuration-policy](#) desde la cuenta de administrador delegado 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 error `ConflictException`, la política de configuración seguirá aplicándose a las cuentas o unidades organizativas de su organización. Para resolver el error, desasocie la política de configuración de estas cuentas o unidades organizativas 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 delegada de administrador de AWS Security Hub, puede desasociar una política de configuración o una configuración autoadministrada de una cuenta, unidad organizativa o raíz. La desasociación conserva la política para su uso en el futuro, pero elimina las asociaciones existentes de cuentas, unidades organizativas o raíz específicas. Solo puede desasociar una configuración aplicada directamente, no una configuración heredada. 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 de AWS Security Hub en <https://console.aws.amazon.com/securityhub/>.
Inicie sesión con las credenciales de la cuenta de administrador delegado de Security Hub 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. Elija 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. Si las configuraciones entran en conflicto con las selecciones actuales, esta acción anula las configuraciones existentes de cualquier cuenta o unidad organizativa que esté dentro del ámbito de aplicación.

API

Desasociación de una cuenta o unidad organizativa de su configuración actual

1. Invoque la API [StartConfigurationPolicyDisassociation](#) desde la cuenta de administrador delegado 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. En Target, indique las cuentas, las unidades organizativas o la raíz que desee desasociar de esta política de configuración.

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 comando [start-configuration-policy-disassociation](#) desde la cuenta de administrador delegado 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. En `target`, indique las cuentas, las unidades organizativas o la raíz que desee desasociar de esta política de configuración.

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, el administrador delegado del Security Hub puede crear políticas de configuración que especifiquen cómo se configuran el Security Hub,

los estándares de seguridad y los controles de seguridad 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 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, al ver los resultados de seguridad, puede descubrir qué estándares y controles son más relevantes para su entorno y configurarlos al mismo tiempo.

La configuración en contexto solo está disponible en la consola de Security Hub.

Desde el punto de vista programático, el administrador delegado debe invocar el [UpdateConfigurationPolicy](#) funcionamiento del Security Hub API 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 de Security Hub en su contexto.

Para configurar un estándar o un control en su contexto (consola)

1. Abra la AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>.
Inicie sesión con las credenciales de la cuenta de administrador delegado de Security Hub 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 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.

Deshabilitación de la configuración centralizada en Security Hub

Cuando deshabilita la configuración centralizada en AWS Security Hub, el administrador delegado pierde la capacidad de configurar Security Hub, los estándares y los controles de seguridad en varias Cuentas de AWS, unidades organizativas (OU) y Regiones de AWS. En su lugar, debe configurar la mayoría de los ajustes por separado para cada cuenta en cada región.

Important

Antes de deshabilitar la configuración centralizada, debe [desasociar las cuentas y las unidades organizativas](#) de su configuración actual, independientemente de si se trata de una política de configuración o de un comportamiento autoadministrado.

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 Security Hub deben configurarse por separado para cada cuenta y región de la organización. El administrador delegado puede habilitar automáticamente Security Hub, 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 las Prácticas recomendadas de seguridad básica de AWS (FSBP) y AWS Foundations Benchmark v1.2.0 de Center for Internet Security (CIS). 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 console

Para deshabilitar la configuración centralizada (consola)

1. Abra la consola de AWS Security Hub en <https://console.aws.amazon.com/securityhub/>.

Inicie sesión con las credenciales de la cuenta de administrador delegado de Security Hub 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 unidades organizativas que se designan como autoadministradas deben desasociarse de su configuración autoadministrada. 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 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 quiere habilitar automáticamente Security Hub en las nuevas cuentas de la organización, establezca el campo AutoEnable en true. De forma predeterminada, el valor de este campo es false y 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 `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 quiere habilitar automáticamente Security Hub en las nuevas cuentas de la organización, incluya el parámetro `auto-enable`. De forma predeterminada, el valor de este parámetro es `no-auto-enable` y 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"}
```

Administración de cuentas de administrador y de miembro en Security Hub

Si su entorno de AWS tiene varias cuentas, puede tratar las cuentas que utilizan AWS Security Hub como cuentas de miembro 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 miembro a un administrador de dos maneras: al integrar Security Hub con AWS Organizations o al enviar y aceptar manualmente las invitaciones de membresía en Security Hub.

Administración de cuentas con AWS Organizations

AWS Organizations es un servicio de administración de cuentas global que permite a los administradores de AWS consolidar y administrar múltiples Cuentas de AWS. 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, Amazon GuardDuty y Amazon Macie. Para obtener más información, consulte la [Guía del usuario de AWS Organizations](#).

Al integrar Security Hub y AWS Organizations, la cuenta de administración de Organizations designa un administrador delegado de Security Hub. Security Hub se habilita automáticamente en la cuenta de administrador delegado en la Región de AWS en la que se designó.

Tras designar un administrador delegado, recomendamos administrar las cuentas en Security Hub con una [configuración centralizada](#). Esta es la forma más eficaz de personalizar Security Hub y garantizar una cobertura de seguridad adecuada para su organización.

La configuración centralizada permite al administrador delegado personalizar Security Hub en varias cuentas y regiones de la organización en lugar de configurarlo región por región. Puede crear una política de configuración para toda la organización o diferentes políticas de configuración para las distintas cuentas y unidades organizativas. Las políticas especifican si Security Hub 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 centralizada, el administrador delegado tiene una capacidad más limitada para configurar Security Hub, lo que se denomina configuración local. En la configuración local, el administrador delegado puede habilitar automáticamente Security Hub 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, 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

Si tiene una cuenta independiente, debe administrar manualmente las cuentas de miembro mediante invitación en Security Hub o si no ha integrado con Organizations. Una cuenta independiente no se puede integrar con Organizations, por lo que es necesario administrarla manualmente. Recomendamos la integración con AWS Organizations y el uso de la configuración centralizada si va a agregar cuentas adicionales en el futuro.

Cuando utiliza la administración manual de cuentas, designa una cuenta como administradora 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 invita a otras cuentas para que sean cuentas de miembro. La relación administrador-miembro se establece cuando una potencial cuenta de miembro 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 Security Hub al configurar parámetros variables para diferentes cuentas. En su lugar, cada cuenta de la organización debe habilitar y configurar Security Hub 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. 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 [Administración de cuentas por invitación en Security Hub](#).

Recomendaciones para entornos de varias cuentas en Security Hub

En la siguiente sección, se resumen algunas restricciones y recomendaciones que se deben tener en cuenta a la hora de administrar las cuentas de miembro en AWS Security Hub.

Número máximo de cuentas miembro

Si utilizas la integración con AWS Organizations, Security Hub admite hasta 10 000 cuentas de miembros por cuenta de administrador delegado en cada una Región de AWS de ellas. Si habilita y administra Security Hub de manera manual, Security Hub admite hasta 1000 invitaciones a cuentas de miembro por cuenta de administrador en cada región.

Creación de relaciones administrador-miembro

Note

Si utilizas la integración 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 de Security Hub habilita una cuenta de la organización, la cuenta no podrá aceptar una invitación de otra cuenta. Si una cuenta ya ha aceptado una invitación, la cuenta de administrador de Security Hub de la organización no podrá habilitarla para la organización. 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 con AWS Organizations, la cuenta de administración de la organización puede designar una cuenta de administrador delegado (DA) para Security Hub. 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, recomendamos que la cuenta de administración de Organizations no sea el administrador delegado.

Le recomendamos que seleccione la misma cuenta de administrador delegado en todas las regiones. Si utiliza la [configuración centralizada](#), Security Hub establece la misma cuenta de administrador delegado en todas las regiones en las que configure Security Hub para su organización.

También le recomendamos que elija la misma cuenta DA en todos los servicios de AWS seguridad y cumplimiento para ayudarle 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 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

Te recomendamos que AWS Organizations utilices invitaciones en lugar de Security Hub para gestionar tus cuentas de miembros.

Coordinar cuentas de administrador en todos los servicios

Security Hub agrupa las conclusiones de varios AWS servicios, como Amazon GuardDuty, Amazon Inspector y Amazon Macie. Security Hub 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. Security Hub 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 Security

Hub, los usuarios de la cuenta A no ven automáticamente GuardDuty los resultados de las cuentas B y C en Security Hub. También se requiere una relación administrador-miembro de Security Hub para estas cuentas.

Para ello, convierta la cuenta A en la cuenta de administrador de Security Hub y habilite las cuentas B y C para que se conviertan en cuentas miembro de Security Hub.

Administración de cuentas de administrador y de miembro de Security Hub con Organizations

Puede realizar la integración AWS Security Hub con Security Hub y AWS Organizations, a continuación, administrarlas para las cuentas de su organización.

Para integrar Security Hub con AWS Organizations, debe crear una organización en AWS Organizations. La cuenta de administración de Organizations designa una cuenta como administrador delegado de Security Hub para la organización. A continuación, el administrador delegado puede habilitar Security Hub para otras cuentas de la organización, agregar esas cuentas como cuentas de miembro del Security Hub y llevar a cabo las acciones permitidas en las cuentas de miembro. El administrador delegado de Security Hub puede habilitar y administrar Security Hub para un máximo de 10 000 cuentas de miembro.

El alcance de las capacidades de configuración del administrador delegado depende de si utiliza la [configuración centralizada](#). Con la configuración central habilitada, no es necesario configurar Security Hub por separado en cada cuenta de miembro y Región de AWS. El administrador delegado puede aplicar ajustes específicos de Security Hub en determinadas cuentas de miembros y unidades organizativas (OUs) de todas las regiones.

La cuenta de administrador delegado de Security Hub puede llevar a cabo las siguientes acciones en las cuentas de miembro:

- Si utiliza la configuración central, configure de forma centralizada el Security Hub para las cuentas de los miembros y OUs cree políticas de configuración del Security Hub. Las políticas de configuración se pueden usar para habilitar y deshabilitar Security Hub y para habilitar y deshabilitar los estándares y controles.
- Tratar automáticamente las nuevas cuentas de la organización como cuentas de miembro de Security Hub a medida que se agregan 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.

- Tratar las cuentas de la organización existentes como cuentas miembro de Security Hub. 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 Security Hub con cuentas de miembros específicas administradas de forma centralizada.

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](#).

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 en las cuentas de administrador y de miembro en Security Hub](#).

En los temas de esta sección se explica cómo integrar Security Hub AWS Organizations y cómo administrar Security Hub 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 con AWS Organizations](#)
- [Habilitación automática de nuevas cuentas de la organización en Security Hub](#)
- [Habilitación manual de Security Hub en las cuentas nuevas de la organización](#)
- [Desasociación de cuentas de miembro de Security Hub de su organización](#)

Integración de Security Hub con AWS Organizations

Para integrar AWS Security Hub y AWS Organizations crear una organización en Organizations y utilizar la cuenta de administración de la organización para designar una cuenta de administrador delegada de Security Hub. Esto habilita Security Hub como un servicio de confianza en Organizations. También habilita Security Hub en la Región de AWS actual para la cuenta de administrador delegado y permite al administrador delegado habilitar Security Hub para las cuentas de los miembros, ver los datos de estas cuentas y llevar a cabo otras [acciones permitidas](#) en ellas.

Si utiliza la [configuración centralizada](#), el administrador delegado también puede crear políticas de configuración de Security Hub que especifiquen cómo se deben configurar el servicio, los estándares y los controles de Security Hub en las cuentas de la organización.

Creación de una organización

Una organización es una entidad que se crea para consolidar la suya y Cuentas de AWS poder administrarla como una sola unidad.

Puede crear una organización mediante la AWS Organizations consola o mediante un comando de AWS CLI o uno de los SDKAPIs. 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

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 Security Hub.

Aunque el Security Hub APIs y la consola permiten que la cuenta de administración de la organización sea el administrador delegado 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 distintos de los usuarios que necesitan acceder a Security Hub para administrar la seguridad.

Le recomendamos que utilice el mismo administrador delegado en todas las regiones. Si opta por la configuración centralizada, Security Hub designa automáticamente el 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 delegado de Security Hub, la cuenta de administración de la organización debe tener permisos para ejecutar las acciones `EnableOrganizationAdminAccount` y `DisableOrganizationAdminAccount` en Security Hub. La cuenta de administración de Organizations también debe contar con permisos administrativos para Organizations.

Para conceder todos los permisos necesarios, adjunta las siguientes políticas gestionadas por Security Hub a la cuenta IAM principal de administración de la organización:

- [AWSSecurityHubFullAccess](#)
- [AWSSecurityHubOrganizationsAccess](#)

Designación del administrador delegado

Para designar la cuenta de administrador delegada de Security Hub, puede usar la consola de Security Hub, Security Hub API o AWS CLI. Security Hub establece al administrador delegado Región de AWS solo en la actual, y debes repetir la acción en otras regiones. Si comienza a utilizar la configuración centralizada, Security Hub 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 Security Hub para designar la cuenta de administrador delegado de Security Hub.

Recomendamos que la cuenta de administración de la organización no sea la misma cuenta de administrador delegado de Security Hub. Sin embargo, si decide usar la cuenta de administración de la organización como administrador delegado de Security Hub, la cuenta de administración debe tener Security Hub habilitado. Si la cuenta de administración no tiene habilitado Security Hub, tendrá que hacerlo manualmente. Security Hub no se puede habilitar automáticamente para la cuenta de administración de la organización.

Debe designar al administrador delegado de Security Hub mediante uno de los siguientes métodos. La designación del administrador delegado del Security Hub con Organizations APIs no se refleja en Security Hub.

Elija el método que prefiera y siga los pasos para designar la cuenta de administrador delegado de Security Hub.

Security Hub console

Para designar al administrador delegado durante el proceso de incorporación

1. Abra la AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>
2. Seleccione Ir a Security Hub. 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 AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>.
2. En el panel de navegación de Security Hub, elija Configuración. A continuación, elija General.
3. Si actualmente hay asignada una cuenta de administrador de Security Hub, debe eliminarla antes de poder designar una nueva cuenta.

En Administrador delegado, para eliminar la cuenta actual, seleccione Eliminar.

4. Ingrese el ID de la cuenta que desea designar como administrador de Security Hub.

Debe designar la misma cuenta de administrador para todas las regiones de Security Hub. Si designa una cuenta diferente de la que ha designado en otras regiones, la consola le mostrará un error.

5. Elija Delegar.

Security Hub API, AWS CLI

Desde la cuenta de administración de la organización, utilice la [EnableOrganizationAdminAccount](#) funcionamiento del Security Hub API. Si está utilizando el AWS

CLI, ejecute el [enable-organization-admin-accountcomando](#). Proporcione el ID de la Cuenta de AWS para el administrador delegado de Security Hub.

El siguiente ejemplo designa al administrador delegado de Security Hub. 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 delegado de Security Hub.

Para cambiar al administrador delegado de Security Hub, primero debe eliminar la cuenta de administrador delegado actual y, luego, designar una nueva.

Warning

Cuando utilizas la [configuración central](#), no puedes usar la consola de Security Hub ni el 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 al administrador delegado del Security Hub, Security Hub 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 de Security Hub para eliminar al administrador delegado en una región, este se elimina en todas las regiones.

El Security Hub API solo elimina la cuenta de administrador delegada del Security Hub de la región en la que se emite la API llamada o el comando. Debe repetir la acción en las demás regiones.

Si utiliza Organizations API para eliminar la cuenta de administrador delegada de Security Hub, se eliminará automáticamente en todas las regiones.

Eliminar al administrador delegado (OrganizationsAPI, AWS CLI)

Puede usar Organizations para eliminar al administrador delegado de Security Hub de 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.

Elige el método que prefieras y sigue las instrucciones para eliminar la cuenta de administrador delegada de Security Hub con AWS Organizations ella.

Organizations API, AWS CLI

Para eliminar al administrador delegado de Security Hub

Desde la cuenta de administración de la organización, utilice [DeregisterDelegatedAdministrator](#) funcionamiento de las OrganizacionesAPI. Si utiliza la AWS CLI, ejecute el comando [deregister-delegated-administrator](#). Proporcione el ID de cuenta del administrador delegado y la entidad principal de servicio para Security Hub, que es `securityhub.amazonaws.com`.

En el siguiente ejemplo, se elimina al administrador delegado de Security Hub. 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
```

Eliminación del administrador delegado (consola de Security Hub)

Puede utilizar la consola de Security Hub para eliminar al administrador delegado de Security Hub de todas las regiones.

Cuando se elimina la cuenta de administrador delegado de Security Hub, las cuentas de los miembros se desvinculan de la cuenta de administrador delegado de Security Hub que se ha eliminado.

Security Hub aún está habilitado en las cuentas de miembro. Se convierten en cuentas independientes hasta que un nuevo administrador de Security Hub las habilite como cuentas de miembro.

Si la cuenta de administración de la organización no es una cuenta habilitada en Security Hub, use la opción de la página Le damos la bienvenida a Security Hub.

Para eliminar la cuenta del administrador delegado de Security Hub de la página Le damos la bienvenida a Security Hub

1. Abra la AWS Security Hub consola 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 del administrador delegado de Security Hub desde la página Configuración

1. Abra la AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>.
2. En el panel de navegación de Security Hub, elija Configuración. A continuación, elija General.
3. En Administrador delegado, seleccione Eliminar.

Eliminar el administrador delegado (Security HubAPI, AWS CLI)

Puede utilizar las operaciones de Security Hub API o Security Hub para eliminar AWS CLI al administrador delegado del Security Hub. Al eliminar al administrador delegado con uno de estos métodos, solo se elimina en la región en la que se emitió la API llamada o el comando. Security Hub no actualiza otras regiones ni elimina la cuenta de administrador delegado en AWS Organizations ellas.

Elija el método que prefiera y siga los pasos para eliminar la cuenta de administrador delegado de Security Hub con el mismo servicio.

Security Hub API, AWS CLI

Para eliminar al administrador delegado de Security Hub

Desde la cuenta de administración de la organización, usa la [DisableOrganizationAdminAccount](#)funcionamiento del Security HubAPI. Si está utilizando el AWS CLI, ejecute el [disable-organization-admin-accountcomando](#) Proporcione el ID de la cuenta del administrador delegado de Security Hub.

En el siguiente ejemplo, se elimina al administrador delegado de Security Hub. 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
```

Desactivación de la integración de Security Hub con AWS Organizations

Una vez integrada una AWS Organizations organización AWS Security Hub, la cuenta de administración de Organizations puede deshabilitar posteriormente la integración. Como usuario de la cuenta de administración de la organización, puede deshabilitar el acceso de confianza de Security Hub en AWS Organizations.

Al deshabilitar el acceso de confianza de Security Hub, ocurre lo siguiente:

- Security Hub pierde su condición de servicio de confianza en AWS Organizations.
- La cuenta de administrador delegado de Security Hub pierde el acceso a la configuración, los datos y los recursos del servicio en todas las cuentas de miembro de todas las Regiones de AWS.
- Si utilizaba la [configuración centralizada](#), Security Hub 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 miembro de Security Hub se convierten en cuentas independientes y retienen su configuración actual. Si Security Hub tenía habilitada una cuenta de miembro en una o más regiones, Security Hub seguirá teniendo habilitada 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 AWS Organizations usuario.

Para deshabilitar el acceso de confianza, puede usar la AWS Organizations consolaAPI, Organizations o el AWS CLI. Solo un usuario de la cuenta de administración de Organizations puede deshabilitar el acceso de Security Hub a los servicios de confianza. 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, recomendamos colaborar con el administrador delegado de su organización para deshabilitar Security Hub en las cuentas de miembro y limpiar los recursos de Security Hub en esas cuentas.

Elija el método que prefiera y siga estos pasos para deshabilitar el acceso de confianza de Security Hub.

Organizations console

Deshabilitación del acceso de confianza de Security Hub

1. Inicie sesión AWS Management Console con las 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.
5. Seleccione Deshabilitar el acceso de confianza.
6. Confirme que desea deshabilitar el acceso de confianza.

Organizations API

Deshabilitación del acceso de confianza de Security Hub

invoque la operación [DisableAWSService Access](#) del AWS Organizations API. Para el parámetro `ServicePrincipal`, especifique la entidad principal de servicio de Security Hub (`securityhub.amazonaws.com`).

AWS CLI

Deshabilitación del acceso de confianza de Security Hub

Ejecute el [disable-aws-service-access](#) comando del AWS Organizations API. Para el parámetro `service-principal`, especifique la entidad principal de servicio de Security Hub (`securityhub.amazonaws.com`).

Ejemplo:

```
aws organizations disable-aws-service-access --service-principal
securityhub.amazonaws.com
```

Habilitación automática de nuevas cuentas de la organización en Security Hub

Cuando se incorporan nuevas cuentas a su organización, se añaden a la lista de la página Cuentas de la AWS Security Hub consola. 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 cuando se unen a la organización. Su estado es No es miembro. La cuenta de administrador delegado puede agregar de manera automática cuentas nuevas como miembros y habilitar Security Hub en estas cuentas cuando se unen a la organización.

Note

Aunque muchas de Regiones de AWS ellas están activas de forma predeterminada en su Cuenta de AWS caso, debe activar algunas regiones de forma manual. En el presente documento estas regiones se denominan regiones de suscripción voluntaria. Para habilitar automáticamente Security Hub en una cuenta nueva en una región de suscripción voluntaria, primero debe activar esa región en la cuenta. Solo el propietario de la cuenta puede activar la región de suscripción voluntaria. Para obtener más información sobre las regiones con las que puedes suscribirte, consulta [Cómo especificar qué regiones puede usar Regiones de AWS tu 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 utiliza la [configuración centralizada](#), puede habilitar automáticamente Security Hub en las cuentas nuevas y las existentes de la organización mediante la creación de una política de configuración en la que Security Hub esté habilitado. 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 Security Hub está habilitado en una unidad organizativa específica, Security Hub se habilita automáticamente en todas las cuentas (existentes y nuevas) que pertenezcan a dicha unidad. Las cuentas nuevas que no pertenecen a la unidad organizativa se autoadministran y no tienen habilitado Security Hub automáticamente. Si asocia a la raíz una política de configuración en la que Security Hub esté habilitado, Security Hub se habilitará 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)

Cuando utiliza la configuración local y activa la habilitación automática de los estándares predeterminados, Security Hub agrega cuentas nuevas de la organización como miembros y habilita Security Hub en ellas en la región actual. Otras regiones no se ven afectadas. Además, al activar la habilitación automática, no se habilita Security Hub en las cuentas de la organización existentes, a menos que ya se hayan agregado como cuentas de miembro.

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) AWS Foundations Benchmark v1.2.0. 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 una configuración centralizada.

OUs

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](#).

Elija el método que prefiera y siga estos pasos para habilitar Security Hub en nuevas cuentas de la organización. Estas instrucciones solo se aplican si utiliza la configuración local.

Security Hub console

Habilitación automática de nuevas cuentas de la organización como cuentas de miembro

1. Abra la AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>.

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

2. En el panel de navegación de Security Hub, en Configuración, elija Configuración.
3. En la sección Cuentas, active Habilitación automática de cuentas.

Security Hub API

Habilitación automática de nuevas cuentas de la organización como cuentas de miembro

Invoque [UpdateOrganizationConfiguration](#)API desde la cuenta de administrador delegado. Defina el campo `AutoEnable` en `true` para habilitar automáticamente Security Hub en las nuevas cuentas de la organización.

AWS CLI

Habilitación automática de nuevas cuentas de la organización como cuentas de miembro

Ejecute el comando [update-organization-configuration](#) desde la cuenta de administrador delegado. Incluya el parámetro `auto-enable` para habilitar automáticamente Security Hub en las nuevas cuentas de la organización.

```
aws securityhub update-organization-configuration --auto-enable
```

Habilitación manual de Security Hub en las cuentas nuevas de la organización

Si no habilita de manera automática Security Hub en las cuentas nuevas de la organización cuando se unen a ella, puede agregar esas cuentas como miembros y habilitar manualmente Security Hub en ellas después de que se unen a la organización. También debes habilitar manualmente el Security Hub si anteriormente te desasociaste de una organización. Cuentas de AWS

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 Security Hub en cuentas de miembros y unidades organizativas específicas (OUs). También puedes habilitar estándares y controles específicos en esas cuentas y OUs.

No puede habilitar Security Hub en una cuenta si ya es una cuenta de miembro de otra organización.

Tampoco puede habilitar Security Hub en una cuenta que esté suspendida. Si intenta habilitar el servicio en una cuenta suspendida, el estado de la cuenta cambia a Cuenta suspendida.

- Si la cuenta no tiene habilitado Security Hub, Security Hub se habilita para 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. Security Hub no se puede habilitar automáticamente para la cuenta de administración de Organizations. Debe habilitar Security Hub de forma manual en la cuenta de administración de Organizations antes de poder agregarla como una cuenta de miembro.

- Si la cuenta ya tiene habilitado Security Hub, Security Hub no hace ningún otro cambio en la cuenta. Solo habilita la membresía.

Para que 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](#).

Elija el método que prefiera y siga los pasos para habilitar una cuenta de organización como cuenta de miembro de Security Hub.

Security Hub console

Habilitación manual de cuentas de la organización como miembros de Security Hub

1. Abra la AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>.

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

2. En el panel de navegación 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 API

Habilitación manual de cuentas de la organización como miembros de Security Hub

Invoque [CreateMembers](#) API 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

Habilitación manual de cuentas de la organización como miembros de Security Hub

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"}]'
```

Desasociación de cuentas de miembro de Security Hub de su organización

Para dejar de recibir y ver los resultados de una cuenta de AWS Security Hub miembro, 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 Security Hub en una o más cuentas de

miembros administradas de forma centralizada. Después de eso, estas cuentas seguirán formando parte de la organización, pero no generarán resultados en 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 desvincular 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 se convierte en una cuenta independiente Cuenta de AWS que ya no se administra mediante la integración de Security Hub con AWS Organizations

Elija el método que prefiera y siga los pasos para desasociar una cuenta de miembro de la organización.

Security Hub console

Desasociación de una cuenta de miembro de la organización

1. Abra la AWS Security Hub consola 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 API

Desasociación de una cuenta de miembro de la organización

Invoque [DisassociateMembersAPI](#) desde la cuenta de administrador delegado. Debe proporcionar las cuentas de los miembros Cuenta de AWS IDs para que se desasocien. Para ver una lista de las cuentas de los miembros, invoca la [ListMembersAPI](#)

AWS CLI

Desasociación de una cuenta de miembro de la organización

Ejecute el comando [>disassociate-members](#) 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, 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 .

Administración de cuentas por invitación en Security Hub

Puede administrar varias AWS Security Hub cuentas de forma centralizada de dos maneras: integrando Security Hub AWS Organizations o enviando y aceptando manualmente las invitaciones de membresía. Debe utilizar el proceso manual si tiene una cuenta independiente o si no quiere integrar su cuenta con Organizations. En la administración manual de cuentas, el administrador 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 de Security Hub puede administrar dicho servicio para hasta 1000 cuentas de miembro basadas en invitaciones.

Note

Si crea una organización basada en invitaciones en Security Hub, puede [hacer la transición con AWS Organizations](#) posteriormente como alternativa. Si tiene más de una cuenta de miembro, le recomendamos que utilice invitaciones AWS Organizations en lugar de Security Hub para administrar sus cuentas de miembro. Para obtener más información,

consulte [Administración de cuentas de administrador y de miembro de Security Hub con 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 activado Security Hub en la región de agregación y en todas las regiones vinculadas para que el administrador pueda ver los resultados desde 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 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 puede que desee consolidar cuentas de varias organizaciones en una sola cuenta de administrador de Security Hub. La cuenta de administrador de Security Hub debe enviar invitaciones a las cuentas que pertenezcan a otras organizaciones.

En la página Configuración de la consola de Security Hub, las cuentas que se agregaron mediante invitación aparecen en la pestaña Cuentas de invitación. Si utiliza [Comprensión de la configuración centralizada en Security Hub](#) e invita 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 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

- [Cómo agregar e invitar cuentas de miembro en Security Hub](#)
- [Responder una invitación para tener una cuenta de miembro de Security Hub](#)
- [Cómo desvincular las cuentas de miembro en Security Hub](#)
- [Cómo eliminar cuentas de miembro en Security Hub](#)
- [Desvincularse de una cuenta de administrador de Security Hub](#)
- [Transición a Organizations para administrar cuentas en Security Hub](#)

Cómo agregar e invitar cuentas de miembro en Security Hub

Note

Te recomendamos que AWS Organizations utilices invitaciones en lugar de Security Hub para gestionar tus cuentas de miembros. Para obtener más información, consulte [Administración de cuentas de administrador y de miembro de Security Hub con Organizations](#).

Su cuenta se convierte en la AWS Security Hub administradora de las cuentas que aceptan su invitación para convertirse en una cuenta de miembro de Security Hub.

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 de Security Hub, también puede agregar cuentas en su lista. En la consola de Security Hub, puede seleccionar las cuentas de forma individual o cargar un archivo .csv 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 console

Cómo agregar cuentas a su lista de cuentas de miembro

1. Abre la AWS Security Hub consola 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 IDs con números no 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 API

Agregación de cuentas a su lista de cuentas de miembro

invoque el [CreateMembers](#) API 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 console

Invitación a potenciales cuentas de miembro

1. Abra la AWS Security Hub consola 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 API

Invitación a potenciales cuentas de miembro

invoque [InviteMembers](#) API desde la cuenta de administrador. Para cada cuenta a la que quieras invitar, debes 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 una invitación para tener una cuenta de miembro de Security Hub.

Note

Te recomendamos que AWS Organizations utilice invitaciones en lugar de Security Hub para gestionar tus cuentas de miembros. Para obtener más información, consulte [Administración de cuentas de administrador y de miembro de Security Hub con Organizations](#).

Puede aceptar o rechazar una invitación para ser AWS Security Hub miembro de una cuenta.

Después de aceptar la invitación, su cuenta se convierte en una cuenta de miembro de Security Hub. La cuenta que envió la invitación pasa a ser su cuenta de administrador de Security Hub. El usuario de la cuenta de administrador puede ver los resultados de su cuenta de miembro en Security Hub.

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.

Antes de poder aceptar o rechazar una invitación, debe activar Security Hub.

Recuerde que todas las cuentas 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

Desde la cuenta de administrador, puede enviar una invitación para tener una cuenta de miembro de Security Hub. 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 console

Aceptación de una invitación a una suscripción

1. Abra la AWS Security Hub consola 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 API

Aceptación de una invitación a una suscripción

Invoca el [AcceptAdministratorInvitation](#) API. 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 de Security Hub sigue empleando `AcceptInvitation`. Con el tiempo, pasará a usar `AcceptAdministratorInvitation`. Se debe seguir utilizando cualquier IAM política que controle específicamente el acceso a esta función `AcceptInvitation`. También debe agregar `AcceptAdministratorInvitation` a sus políticas los permisos correctos una vez que la consola comience a utilizar `AcceptAdministratorInvitation`.

Cómo rechazar una invitación

Puede rechazar una invitación para tener una cuenta de miembro de Security Hub. Cuando rechaza una invitación en la consola de Security Hub, su cuenta se marca como Dada de baja en la lista de cuentas de miembro de la cuenta de administrador. El estado Dado de baja solo aparece cuando se inicia sesión en la consola 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 console

Rechazo de una invitación a una membresía

1. Abra la AWS Security Hub consola 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 API

Rechazo de una invitación a una membresía

Invoca el [DeclineInvitations](#) API. 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"
```

Cómo desvincular las cuentas de miembro en Security Hub

Note

Te recomendamos que AWS Organizations utilice invitaciones en lugar de Security Hub para gestionar tus cuentas de miembros. Para obtener más información, consulte [Administración de cuentas de administrador y de miembro de Security Hub con Organizations](#).

Una cuenta de AWS Security Hub administrador puede desasociar la cuenta de un 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 console

Desasociación de una cuenta de miembro invitada manualmente

1. Abre la AWS Security Hub consola 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 API

Desasociación de una cuenta de miembro invitada manualmente

Invoque [DisassociateMembers](#) API 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 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"
```

Cómo eliminar cuentas de miembro en Security Hub

Note

Te recomendamos que AWS Organizations utilices invitaciones en lugar de Security Hub para gestionar tus cuentas de miembros. Para obtener más información, consulte [Administración de cuentas de administrador y de miembro de Security Hub con Organizations](#).

Como cuenta de AWS Security Hub administrador, puede eliminar las cuentas de los miembros que se agregaron mediante 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 puedes 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 invitadas manualmente.

Security Hub console

Eliminación de una cuenta de miembro invitada manualmente

1. Abre la AWS Security Hub consola 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 API

Eliminación de una cuenta de miembro invitada manualmente

Invoque [DeleteMembersAPI](#) 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 miembros, invoca la [ListMembersAPI](#).

AWS CLI

Eliminación de una cuenta de miembro invitada manualmente

Ejecute el comando [delete-members](#) 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, ejecute el comando [list-members](#).

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

Ejemplo

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

Desvincularse de una cuenta de administrador de Security Hub

Note

Te recomendamos que AWS Organizations utilices invitaciones en lugar de Security Hub para gestionar tus cuentas de miembros. Para obtener más información, consulte [Administración de cuentas de administrador y de miembro de Security Hub con Organizations](#).

Si su cuenta se agregó como cuenta de AWS Security Hub miembro por invitación, puede desvincular la cuenta de miembro de la cuenta de administrador. Una vez que desvincula una cuenta de miembro, Security Hub 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 Security Hub puede desasociar las cuentas de miembro 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 console

Cómo desvincularse de su cuenta de administrador

1. Abre la AWS Security Hub consola 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 API

Desasociación de su cuenta de administrador

Invoca el [DisassociateFromAdministratorAccount](#) API.

AWS CLI

Desasociación de su cuenta de administrador

Ejecute el comando [disassociate-from-administrator-account](#).

```
aws securityhub disassociate-from-administrator-account
```

Note

La consola de Security Hub sigue empleando `DisassociateFromMasterAccount`. Con el tiempo, pasará a usar `DisassociateFromAdministratorAccount`. Se debe seguir utilizando cualquier IAM política que controle específicamente el acceso a esta función. `DisassociateFromMasterAccount` También debe agregar `DisassociateFromAdministratorAccount` a sus políticas los permisos correctos una vez que la consola comience a utilizar `DisassociateFromAdministratorAccount`.

Transición a Organizations para administrar cuentas en Security Hub

Al administrar las cuentas manualmente en AWS Security Hub, debe invitar a las potenciales cuentas de miembro y configurarlas por separado en cada Región de AWS.

Al integrar Security Hub y AWS Organizations, puede eliminar la necesidad de enviar invitaciones y obtener un mayor control sobre cómo se configura y personaliza Security Hub en su organización. Por este motivo, recomendamos utilizar AWS Organizations en lugar de las invitaciones de Security Hub para administrar las cuentas de miembro. Para obtener más información, consulte [Administración de cuentas de administrador y de miembro de Security Hub con Organizations](#).

Es posible utilizar un enfoque combinado en el que se utiliza la integración de AWS Organizations, pero también se pueden invitar manualmente a cuentas ajenas a la organización. Sin embargo, recomendamos utilizar exclusivamente la integración de Organizations. La [configuración centralizada](#), una característica que le ayuda a administrar 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 con AWS Organizations

En primer lugar, debe integrar Security Hub 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.
- Con su cuenta de administración de Organizations, designe una cuenta como administrador delegado de Security Hub.

Note

La cuenta de administración de Organizations no se puede establecer como cuenta de administrador delegado.

Para obtener instrucciones detalladas, consulte [Integración de Security Hub con AWS Organizations](#).

Al completar los pasos anteriores, concederá un [acceso de confianza](#) a Security Hub en AWS Organizations. También habilita Security Hub en la Región de AWS actual de la cuenta del administrador delegado.

El administrador delegado puede administrar la organización en Security Hub, principalmente, mediante la agregación de cuentas de la organización como cuentas de miembro de Security Hub. El administrador también puede acceder a determinados ajustes, datos y recursos de Security Hub para esas cuentas.

Al hacer la transición a la administración de cuentas mediante Organizations, las cuentas basadas en invitaciones no se convierten automáticamente en miembros de Security Hub. Solo las cuentas que agregue a su nueva organización pueden convertirse en miembros de Security Hub.

Tras activar la integración, puede administrar las cuentas con Organizations. Para obtener más información, consulte [Administración de cuentas de administrador y de miembro de Security Hub con Organizations](#). La administración de cuentas varía en función del tipo de configuración de la organización.

Acciones permitidas en las cuentas de administrador y de miembro en Security Hub

Las cuentas de administrador y miembro tienen acceso a AWS Security Hub las acciones 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 en función de si se realiza la integración AWS Organizations y del tipo de configuración que utilice la organización. Para obtener más información acerca de la diferencia la configuración local y centralizada, consulte [Administración de cuentas con AWS Organizations](#).

Security Hub no copia los resultados de las cuentas de miembro en la cuenta de administrador. En Security Hub, todos los resultados 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](#).

Esta tabla refleja los permisos predeterminados para las cuentas de administrador y de miembro. Puede usar IAM políticas personalizadas para restringir aún más el acceso a las características y funciones de Security Hub. Para obtener orientación y ejemplos, consulte la entrada del blog [Alineación de IAM las políticas con los perfiles de los usuarios para AWS Security Hub](#).

Acciones permitidas si integra con Organizations y usa la configuración centralizada

Las cuentas de administrador y de miembro pueden acceder a las acciones de Security Hub de la siguiente manera si integra con Organizations y usa la configuración centralizada.

Acción	Cuenta de administrador delegado para Security Hub	Cuenta de miembro administrada de forma centralizada	Cuenta de miembro autoadministrada
Creación y administración de políticas de configuración de Security Hub	Para cuentas administradas automáticamente y de forma centralizada	–	–
Visualización de cuentas de la organización	Cualquiera	–	–
Desvincular cuenta de miembro	Cualquiera	–	–
Eliminar cuenta de miembro	Cualquier cuenta que no sea de una organización	–	–
Deshabilitar Security Hub	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

Acción	Cuenta de administrador delegado para Security Hub	Cuenta de miembro administrada de forma centralizada	Cuenta de miembro autoadministrada
Activación o desactivación de los resultados de control consolidados	Cualquiera	–	–
Habilitar y deshabilitar estándares	Para cuentas actuales y cuentas administradas de forma centralizada	–	Actuales
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 de miembro pueden acceder a las acciones de Security Hub de la siguiente manera si integra con Organizations y usa la configuración local.

Acción	Cuenta de administrador delegado para Security Hub	Cuenta de miembro
Creación y administración de políticas de configuración de Security Hub	–	–
Visualización de cuentas de la organización	Cualquiera	–
Desvincular cuenta de miembro	Cualquiera	–
Eliminar cuenta de miembro	–	–
Deshabilitar Security Hub	–	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

Acción	Cuenta de administrador delegado para Security Hub	Cuenta de miembro
Habilitación automática de Security Hub y los estándares predeterminados en las nuevas cuentas de la organización	Para cuentas actuales y cuentas nuevas 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 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 de Security Hub	Cuenta de miembro
Creación y administración de políticas de configuración de Security Hub	–	–
Visualización de cuentas de la organización	Cualquiera	–
Desvincular cuenta de miembro	Cualquiera	Actuales
Eliminar cuenta de miembro	Cualquiera	–
Deshabilitar Security Hub	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
Habilitación automática de Security Hub y los estándares predeterminados en	–	–

Acción	Cuenta de administrador de Security Hub	Cuenta de miembro
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

Efecto de las acciones de la cuenta en los datos de Security Hub

Estas acciones de la cuenta tienen los siguientes efectos en los datos de AWS Security Hub.

Security Hub desactivado

Si utiliza la [configuración centralizada](#), el administrador delegado puede crear políticas de configuración de Security Hub que deshabiliten AWS Security Hub en cuentas y unidades organizativas (OU) específicas. En este caso, Security Hub está deshabilitado en las cuentas y unidades organizativas especificadas de su región de origen y en cualquier región vinculada.

Si no utiliza la configuración centralizada, debe deshabilitar Security Hub por separado en cada cuenta y región en la que lo haya habilitado.

No se generan nuevos resultados para la cuenta de administrador si Security Hub está deshabilitado en la cuenta de administrador. Tampoco puede usar la configuración centralizada si Security Hub está deshabilitado en la cuenta de administrador delegado. Los hallazgos existentes se suprimen al cabo de 90 días.

Las integraciones con otros Servicios de AWS se eliminan.

Los estándares de seguridad y controles habilitados se deshabilitan.

Se retienen otros datos y opciones de configuración de Security Hub, como las asociaciones de cuentas de miembro, acciones personalizadas, información y suscripciones a productos de terceros.

Cuenta miembro disociada de la cuenta de administrador

Cuando una cuenta de miembro se desasocia de la cuenta de administrador, esta pierde el permiso para ver los resultados en la cuenta de miembro. Sin embargo, Security Hub continúa habilitado en las dos cuentas.

Si utiliza la configuración centralizada, el administrador delegado no puede configurar Security Hub para una cuenta de miembro que se haya desasociado de la cuenta de administrador delegado.

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, una vez que se han desvinculado las cuentas, es posible que se utilice una acción personalizada en la cuenta de administrador como patrón de eventos en una regla de Amazon EventBridge. 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 Security Hub, las cuentas eliminadas tienen el estado Desasociada.

La cuenta miembro se elimina de una organización

Cuando se elimina una cuenta de miembro de una organización, la cuenta de administrador de Security Hub pierde el permiso para ver los resultados de la cuenta de miembro. Sin embargo, Security Hub sigue habilitado en ambas cuentas con la misma configuración que tenían antes de la eliminación.

Si utiliza la configuración centralizada, no podrá configurar 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 Security Hub, las cuentas eliminadas tienen el estado Eliminada.

La cuenta está suspendida.

Cuando se suspende una cuenta en AWS, la cuenta pierde el permiso para ver sus resultados en Security Hub. No se generan nuevos resultados para esa cuenta. La cuenta de administrador de una cuenta suspendida puede ver los resultados de la cuenta existente.

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 sus permisos de Security Hub. Si el estado de la cuenta de miembro es Cuenta suspendida, la cuenta del administrador debe habilitar la cuenta manualmente.


La cuenta se cierra

Cuando se cierra una Cuenta de AWS, Security Hub responde de la siguiente manera.

Security Hub retiene cada resultado existente en la cuenta durante 90 días a partir del valor más reciente del campo `UpdatedAt` de ASFF. El resultado se retiene durante 90 días a partir de esta fecha, incluso si Security Hub está deshabilitado. Después de los 90 días, Security Hub eliminará de forma permanente los resultados de la cuenta.

- Si desea retener los resultados durante más de 90 días, puede utilizar una acción personalizada con una regla de Amazon EventBridge para almacenar los resultados en un bucket de Amazon S3. Luego, cuando vuelva a abrir la cuenta cerrada, Security Hub restablecerá los resultados de la cuenta.
- Si la cuenta es de administrador de Security Hub, se eliminará como administrador y se eliminarán todas las cuentas de miembro. Si la cuenta es una cuenta de miembro, se desvinculará y se eliminará como miembro de la cuenta del administrador de Security Hub.

- Para obtener más información, consulte [Cierre de una cuenta](#) en la Guía del usuario de Administración de facturación y costos de AWS.

 Important

Para los clientes de las regiones AWS GovCloud (US):

- Antes de cerrar la cuenta, realice un copia de seguridad y, luego, elimine los datos de la política y los demás recursos de la cuenta. Ya no tendrá acceso a ellos después de cerrar la cuenta.

Descripción de agregación entre regiones en Security Hub

Note

La región de agregación ahora se denomina región de origen. Algunas operaciones de la API de Security Hub siguen utilizando el antiguo término región de agregación.

Al usar la agregación entre regiones en AWS Security Hub, puede agregar resultados, encontrar actualizaciones, hallazgos, y controlar los estados de cumplimiento y las puntuaciones de seguridad de varias Regiones de AWS en una sola región de origen. A continuación, puede gestionar 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 resultados, las actualizaciones de resultados y los hallazgos en todas las AWS GovCloud (US). En concreto, solo puede agregar resultados, actualizaciones y hallazgos entre AWS GovCloud (EE. UU. Este) y AWS GovCloud (Oeste). 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 centralizada, el administrador delegado de Security Hub puede configurar 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, agregue los siguientes permisos a su rol de IAM que usa Security Hub:

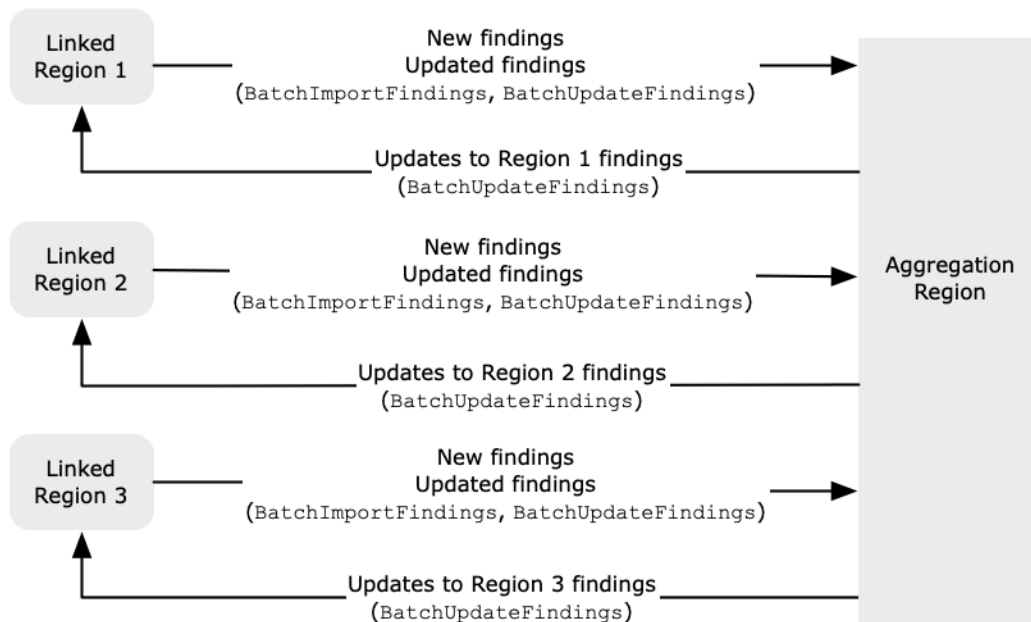
- [ListSecurityControlDefinitions](#)
- [BatchGetStandardsControlAssociations](#)
- [BatchUpdateStandardsControlAssociations](#)

Tipos de datos que se agregan

Cuando la agregación entre regiones está habilitada con una o más regiones vinculadas, Security Hub 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 que se muestran en la lista anterior, Security Hub 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 de Security Hub. No se le cobrará nada cuando Security Hub 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.

Security Hub solo agrega datos de las regiones en las que haya alguna cuenta que tenga activado Security Hub. Security Hub no se habilita automáticamente para ninguna 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 replica los datos que la cuenta de administrador genera en todas las regiones vinculadas a la región de origen. Además, Security Hub identifica las cuentas de miembros que están asociadas a ese administrador, y cada cuenta de miembro hereda la configuración de agregación entre regiones del administrador. Security Hub 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 Security Hub, debe iniciar sesión en la región de origen para ver los datos agregados de todas las cuentas de miembros y las regiones vinculadas.

Como cuenta de miembro de Security Hub, debe iniciar sesión en la región de origen para ver los datos agregados de su cuenta desde 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 de forma manual a cuentas de miembros o actuar como administradora delegada de una organización integrada con 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 de miembro debe tener activado Security Hub en la región de origen y en todas las regiones vinculadas para que el administrador pueda ver los resultados de la cuenta de miembro. Si no utiliza la región de origen para otros fines, puedes deshabilitar los estándares e integraciones del 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 centralizada es una característica opcional de AWS Security Hub que puede utilizar si se integra con AWS Organizations. Con la configuración centralizada, la cuenta de administrador delegado puede configurar el servicio de Security Hub, sus estándares y controles en varias cuentas y unidades organizativas (OU) de la organización. Para configurar cuentas y unidades organizativas, el administrador delegado crea políticas de configuración de Security Hub. Las políticas de configuración se pueden utilizar para definir si se habilita o deshabilita Security Hub y qué estándares y controles están habilitados. El administrador delegado asocia las políticas de configuración a cuentas, unidades organizativas específicas o a la raíz (toda la organización).

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 [Comprensión de la configuración centralizada en Security Hub](#).

Habilitación de agregación entre regiones

Note

La región de agregación ahora se denomina región de origen. Algunas operaciones de la API de Security Hub siguen utilizando el antiguo término región de agregación.

Debe habilitar la agregación entre regiones desde la Región de AWS que designe como la región de origen.

Para habilitar la agregación entre regiones, debe crear un recurso de Security Hub que se denomina agregador de resultados. El recurso del agregador de resultados especifica su región de origen y las regiones vinculadas (si las hubiera).

No puede usar una 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 comience a admitirlas y se haya suscrito a ellas.

Security Hub console

Cómo habilitar la agregación entre regiones

1. Abra la consola de AWS Security Hub en <https://console.aws.amazon.com/securityhub/>.
2. Mediante el selector de Región de AWS, inicie sesión en la región que desee utilizar como región de agregación.
3. En el menú de navegación 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 y usted se suscribe a ellas, seleccione Vincular futuras regiones.
8. Seleccione Guardar.

Security Hub API

Desde la región que desee utilizar como región de origen, use la operación [CreateFindingAggregator](#) de la API de Security Hub. Si usa la AWS CLI, ejecute el comando [create-finding-aggregator](#).

En `RegionLinkingMode`, elija una de las siguientes opciones:

- `ALL_REGIONS`: Security Hub agrega datos de todas las regiones. Security Hub también agrega datos de nuevas regiones a medida que son compatibles y usted se suscribe a ellas.
- `ALL_REGIONS_EXCEPT_SPECIFIED`: Security Hub agrega datos de todas las regiones, excepto de las regiones que desee excluir. Security Hub también agrega datos de nuevas regiones a medida que son compatibles y usted se suscribe a ellas. Utilice `Regions` para proporcionar la lista de regiones que se van a excluir de la agregación.
- `SPECIFIED_REGIONS`: Security Hub agrega datos de una lista seleccionada de regiones. Security Hub no agrega automáticamente los datos de las nuevas regiones. Se utiliza `Regions` para proporcionar la lista de regiones desde las que agregar.

- `NO_REGIONS`: Security Hub no agrega datos porque no selecciona 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
```

Visualización de la configuración de agregación entre regiones

Note

La región de agregación ahora se denomina región de origen. Algunas operaciones de la API de Security Hub siguen utilizando el antiguo término región de agregación.

Puede ver la configuración actual de agregación entre regiones en AWS Security Hub desde cualquier Región de AWS. La configuración incluye la región de origen, las regiones vinculadas (si las hay) y la posibilidad de vincular automáticamente nuevas regiones a medida que Security Hub las admita.

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 console

Para ver la configuración de agregación entre regiones (consola)

1. Abra la consola de AWS Security Hub 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
- Si desea agregar automáticamente los resultados, los hallazgos, los estados de control y las puntuaciones de seguridad de las nuevas regiones compatibles con Security Hub y a las que se suscribe.
- La lista de regiones vinculadas (si se selecciona alguna)

Security Hub API

Para ver la configuración de agregación entre regiones (API de Security Hub)

Use la operación [GetFindingAggregator](#) de la API de Security Hub. Si usa la AWS CLI, ejecute el comando [get-finding-aggregator](#).

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 de Security Hub siguen utilizando el antiguo término región de agregación.

Puede actualizar su configuración actual de agregación entre regiones en AWS Security Hub cambiando las regiones vinculadas o la región de origen actual. También puede cambiar si desea agregar automáticamente los datos nuevos de las Regiones de AWS que admiten 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 haya introducido el 20 de marzo de 2019 o después se consideran regiones opcionales.

Cuando deja de agregar datos de una región vinculada, AWS Security Hub no elimina ningún dato agregado existente de esa región que sea accesible 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 console

Para cambiar las regiones vinculadas

1. Abra la consola de AWS Security Hub en <https://console.aws.amazon.com/securityhub/>.
Inicie sesión en la región de agregación actual.
2. En el menú de navegación 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 vincula automáticamente las nuevas regiones a medida que agrega compatibilidad para ellas y usted se suscribe a ellas.
6. Seleccione Guardar.

Security Hub API

Utilice la operación [UpdateFindingAggregator](#). Si usa la AWS CLI, ejecute el comando [update-finding-aggregator](#). Para identificar el agregador de resultados, debe proporcionar el ARN de este. Para obtener el ARN del agregador de resultados, utilice la operación [ListFindingAggregators](#) 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 de Security Hub siguen utilizando el antiguo término región de agregación.

Si desea que AWS Security Hub no agregue datos, puede eliminar su agregador de resultados. Como alternativa, puede conservar su agregador de resultados, pero no vincular ninguna Regiones de AWS a la región de origen mediante la actualización del 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 resultados, Security Hub 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 las regiones distintas de la región de origen, el panel Agregación de resultados en la consola 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 console

Para detener la agregación entre regiones (consola)

1. Abra la consola de AWS Security Hub 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 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 Guardar.

7. En el cuadro de diálogo de confirmación, en el campo de confirmación, escriba **Confirm**.
8. Elija Confirmar.

Security Hub API

Use la operación [DeleteFindingAggregator](#) de la API de Security Hub. Si utiliza la AWS CLI, ejecute el comando [delete-finding-aggregator](#).

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

En AWS Security Hub, un estándar de seguridad es un conjunto de requisitos basados en marcos regulatorios, mejores prácticas del sector o políticas de la empresa.

Para obtener una lista de los estándares disponibles en Security Hub y los controles que se les aplican, consulte [Referencia de estándares de Security Hub](#). La página Security standards de la consola de Security Hub también muestra todos los estándares de seguridad compatibles en Security Hub y la información a continuación:

- Una descripción de cada estándar compatible
- El estado de habilitación del estándar
- Una lista de los controles habilitados actualmente en el estándar y el estado general de esos controles en función del estado de cumplimiento de sus resultados
- Una lista de los controles que se aplican al estándar, pero que están deshabilitados actualmente
- Una puntuación de seguridad para el estándar

Cuando habilita un estándar, Security Hub habilita automáticamente todos los controles que se aplican al estándar. Puede deshabilitar y volver a habilitar controles según sea necesario. Security Hub ejecuta controles de seguridad en los controles habilitados. Los controles de seguridad dan lugar a los resultados de Security Hub. Cuando deshabilita un estándar, Security Hub deja de ejecutar controles de seguridad en los controles que forman parte de ese estándar. Ya no se generan resultados.

Puede habilitar los estándares de forma individual para una sola cuenta y Región de AWS. Sin embargo, para ahorrar tiempo y reducir desviaciones de configuración en entornos con varias cuentas o regiones, recomendamos utilizar una [configuración centralizada](#) para habilitar los estándares. Con la configuración centralizada, el administrador delegado de Security Hub puede crear políticas que especifican cómo debe configurarse un estándar en varias cuentas y regiones. Para obtener más información acerca de cómo habilitar un estándar, consulte [Habilitación de un estándar de seguridad en Security Hub](#).

Security Hub genera una puntuación de seguridad para cada estándar en función del estado de los controles que se aplican al estándar. Si inicia sesión en una cuenta de administrador, las puntuaciones de seguridad reflejan los estados de control de todas las cuentas de los miembros. Si ha establecido una región de agregación, sus puntuaciones de seguridad reflejan los estados de

control en todas las regiones vinculadas. Para obtener más información, consulte [Método de cálculo de las puntuaciones de seguridad](#).

Referencia de estándares de Security Hub

En AWS Security Hub, un estándar de seguridad es un conjunto de requisitos basados en los marcos normativos, las mejores prácticas del sector o las políticas de la empresa. Security Hub asigna estos requisitos a los controles y realiza controles de seguridad en los controles para evaluar si se cumplen los requisitos de un estándar. Un estándar incluye varios controles.

Un control individual puede pertenecer a uno o varios estándares. Si activa los resultados de control consolidados, Security Hub genera un único resultado por control de seguridad, incluso cuando un control forma parte de varios estándares habilitados. Para obtener más información, consulte [Resultados de control consolidados](#).

Actualmente, Security Hub es compatible con los estándares de seguridad detallados en esta sección. Recomendamos habilitar los estándares que sean relevantes para las necesidades empresariales, para el sector o el caso de uso. Este es un breve resumen de los estándares compatibles. En la siguiente lista, elija un estándar para ver más detalles sobre él y los controles que se aplican a él.

- [AWS Foundational Security Best Practices v1.0.0 \(FSBP\)](#): desarrollado por profesionales del sector AWS y desarrollado por profesionales del sector, el FSBP es una recopilación de las mejores prácticas para organizaciones, independientemente de su sector o tamaño.
- Punto de [referencia básico del Center for Internet Security \(CIS\): proporciona pautas de configuración de AWS los recursos](#). AWS
- [SP 800-53 Rev. 5 del Instituto Nacional de Estándares y Tecnología \(NIST\)](#): generalmente se aplica a las agencias u organizaciones federales que trabajan con agencias federales o sistemas de información federales.
- [Estándar de seguridad de datos para la industria de tarjetas de pago \(PCI DSS\)](#): se aplica a las organizaciones que almacenan, procesan o transmiten datos de titulares de tarjetas.
- [AWS Estándar de etiquetado de recursos](#): le ayuda a realizar un seguimiento de las etiquetas que aplica a sus recursos. AWS
- [Estándar gestionado por el servicio: AWS Control Tower](#) — Se aplica a los usuarios de Security Hub y AWS Control Tower que desean habilitar controles proactivos y de detección.

Para obtener instrucciones sobre cómo habilitar un estándar, consulte [Habilitación de un estándar de seguridad en Security Hub](#).

Los estándares y controles de Security Hub no garantizan el cumplimiento de ningún marco regulatorio o auditoría. Por el contrario, los controles proporcionan una forma de monitorear el estado actual de sus Cuentas de AWS y sus recursos.

AWS Estándar básico de mejores prácticas de seguridad v1.0.0 (FSBP)

El estándar AWS fundamental de mejores prácticas de seguridad es un conjunto de controles que detectan cuándo usted Cuentas de AWS y sus recursos se desvían de las mejores prácticas de seguridad.

El estándar le permite evaluar continuamente todas sus cargas de trabajo Cuentas de AWS y las de trabajo para identificar rápidamente las áreas en las que se desvían de las mejores prácticas. Proporciona orientación práctica y normativa sobre cómo mejorar y mantener la política de seguridad de su organización.

Los controles incluyen las mejores prácticas de seguridad para los recursos de varios Servicios de AWS. A cada control también se le asigna una categoría que refleja la característica de seguridad a la que se aplica. Para obtener más información, consulte [the section called “Categorías de control”](#).

Controles que se aplican al estándar FSBP

[\[Account.1\] La información de contacto de seguridad debe proporcionarse para una Cuenta de AWS](#)

[\[ACM.1\] Los certificados importados y ACM emitidos deben renovarse después de un período de tiempo específico](#)

[\[ACM.2\] RSA los certificados gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)

[\[APIGateway.1\] La API puerta de enlace REST y el registro de WebSocket API ejecuciones deben estar habilitados](#)

[\[APIGateway.2\] REST API Las etapas de la API puerta de enlace deben configurarse para usar SSL certificados para la autenticación de fondo](#)

[\[APIGateway.3\] REST API Las etapas de API Gateway deben tener habilitado el AWS X-Ray rastreo](#)

[\[APIGateway.4\] La API puerta de enlace debe estar asociada a una web WAF ACL](#)

[\[APIGateway.5\] Los datos de la REST API caché 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 de API Gateway V2](#)

[\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)

[\[AppSync.2\] AWS AppSync debe tener activado el registro a nivel de campo](#)

[\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves API](#)

[\[AppSync.6\] AWS AppSync API Las cachés 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 controles de ELB estado](#)

[\[AutoScaling.2\] 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](#)

[Los puntos de recuperación de \[Backup.1\] AWS Backup deben estar cifrados en reposo](#)

[\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)

[\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)

[\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)

[\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)

[\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)

[\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)

[\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)

[\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)

[\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)

[\[CloudTrail.1\] CloudTrail debe habilitarse y configurarse con al menos un registro multirregional que incluya eventos de administración de lectura y escritura](#)

[\[CloudTrail.2\] CloudTrail debe tener activado el cifrado en reposo](#)

[\[CloudTrail.4\] La validación del 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](#)

[\[DataFirehose.1\] Los flujos de entrega de Firehose deben estar cifrados en reposo](#)

[\[DataSync.1\] Las tareas de DataSync deben tener el registro habilitado](#)

[\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)

[\[DMS.6\] las instancias de DMS replicación deben tener habilitada la actualización automática de las versiones secundarias](#)

[\[DMS.7\] las tareas de DMS replicación de la base de datos de destino deben tener habilitado el registro](#)

[\[DMS.8\] las tareas de DMS replicación de la base de datos de origen deben tener el registro activado](#)

[\[DMS.9\] Los DMS puntos finales deben utilizar SSL](#)

[\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización IAM](#)

[\[DMS.11\] DMS Los puntos finales de MongoDB deberían tener habilitado un mecanismo de autenticación](#)

[\[DMS.12\] DMS Los puntos finales de Redis deberían estar habilitados OSS TLS](#)

[\[DocumentDB.1\] 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 \(\) deben cifrarse en reposo DAX](#)

[\[DynamoDB.6\] 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 deberían poder restaurarse públicamente](#)

[\[EC2.2\] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente](#)

[\[EC2.3\] Los volúmenes adjuntos de Amazon EBS deben cifrarse en reposo](#)

[\[EC2.4\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)

[\[EC2.6\] El registro de flujo de VPC debe estar habilitado en todas 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](#)

[\[EC2.15\] EC2 Las subredes de Amazon no deberían 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 deberían permitir el tráfico entrante sin restricciones en los puertos autorizados](#)

[\[EC2.19\] Los grupos de seguridad no deberían permitir el acceso sin restricciones a los puertos de alto riesgo](#)

[\[EC2.20\] Los dos túneles VPN de una conexión AWS Site-to-Site VPN deben estar activos](#)

[\[EC2.21\] La red no ACLs debe permitir la entrada desde el 0.0.0.0/0 al puerto 22 o al puerto 3389](#)

[\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)

[\[EC2.24\] No se deben usar 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](#)

[\[EC2.51\] Los puntos finales de 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 utilizar la versión 2 \(\) del Servicio de Metadatos de Instancia IMDSv2](#)

[\[EC2.171\] Las conexiones EC2 VPN deben tener el registro activado](#)

[\[EC2.172\] La configuración del acceso público al bloqueo de EC2 VPC debería bloquear el tráfico de las puertas de enlace de Internet](#)

[\[ECR.1\] Los repositorios ECR privados deben tener configurado el escaneo de imágenes](#)

[\[ECR.2\] Los repositorios ECR privados deben tener configurada la inmutabilidad de las etiquetas](#)

[\[ECR.3\] ECR Los repositorios deben tener configurada al menos una política de ciclo de vida](#)

[\[ECS.1\] Las definiciones de ECS tareas de Amazon deben tener modos de red seguros y definiciones de usuario.](#)

[\[ECS.2\] ECS los servicios no deberían tener direcciones IP públicas asignadas automáticamente](#)

[\[ECS.3\] las definiciones de ECS tareas no deben compartir el espacio de nombres del proceso del host](#)

[\[ECS.4\] los ECS contenedores deberían ejecutarse sin privilegios](#)

[\[ECS.5\] ECS Los contenedores 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 ECS tareas deben tener una configuración de registro](#)

[\[ECS.10\] Los servicios de ECS Fargate deberían ejecutarse en la última versión de la plataforma Fargate](#)

[\[ECS.12\] ECS los clústeres deben usar Container Insights](#)

[\[ECS.16\] Los conjuntos de ECS tareas 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](#)

[\[EFS.2\] EFS Los volúmenes de Amazon deberían estar en los planes de respaldo](#)

[\[EFS.3\] los puntos de EFS acceso deben establecer un directorio raíz](#)

[\[EFS.4\] los puntos de EFS acceso deben imponer la identidad de un usuario](#)

[\[EFS.6\] Los destinos de EFS montaje no deben estar asociados a una subred pública](#)

[\[EFS.7\] los sistemas de EFS archivos deben tener habilitadas las copias de seguridad automáticas](#)

[\[EFS.8\] los sistemas de EFS archivos deben cifrarse en reposo](#)

[\[EKS.1\] Los puntos finales de los EKS clústeres no deben ser de acceso público](#)

[\[EKS.2\] EKS los clústeres deberían ejecutarse en una versión compatible de Kubernetes](#)

[\[EKS.3\] los EKS clústeres deben usar secretos de Kubernetes cifrados](#)

[\[EKS.8\] EKS los clústeres deben tener habilitado el registro de auditoría](#)

[\[ElastiCache.1\] Los clústeres ElastiCache \(RedisOSS\) 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 \(RedisOSS\) de versiones anteriores deberían tener Redis activado OSS AUTH](#)

[\[ElastiCache.7\] 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](#)

[\[ELB.1\] Application Load Balancer debe configurarse para redirigir todas las HTTP solicitudes a HTTPS](#)

[\[ELB.2\] Los balanceadores de carga clásicos con HTTPS listenersSSL/deben usar un certificado proporcionado por AWS Certificate Manager](#)

[\[ELB.3\] Los oyentes de Classic Load Balancer deben configurarse con o con terminación HTTPS TLS](#)

[\[ELB.4\] Application Load Balancer debe configurarse para eliminar los encabezados http no válidos](#)

[\[ELB.5\] El registro de aplicaciones y balanceadores de carga clásicos debe estar habilitado](#)

[\[ELB.6\] Los balanceadores de carga de aplicaciones, puertas de enlace y redes deben tener habilitada la protección contra eliminaciones](#)

[\[ELB.7\] Los balanceadores de carga clásicos deberían tener habilitado el drenaje de conexiones](#)

[\[ELB.8\] Los balanceadores de carga clásicos que utilizan dispositivos de SSL escucha deben usar una política de seguridad predefinida que tenga una larga duración AWS Config](#)

[\[ELB.9\] Los balanceadores de carga clásicos deberían tener activado el balanceo de cargas entre zonas](#)

[\[ELB.10\] Classic Load Balancer debe abarcar varias zonas de disponibilidad](#)

[\[ELB.12\] Application Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)

[\[ELB.13\] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad](#)

[\[ELB.14\] El Classic Load Balancer 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](#)

[\[EMR.2\] 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](#)

[\[FSx.1\] FSx para sistemas de ZFS archivos abiertos, debe configurarse para copiar etiquetas a copias de seguridad y volúmenes](#)

[\[FSx.2\] FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad](#)

[\[Glue.3\] Las transformaciones AWS Glue de aprendizaje automático deben cifrarse en reposo](#)

[\[GuardDuty.1\] GuardDuty debe estar activado](#)

[\[GuardDuty.5\] La supervisión del registro de GuardDuty EKS auditoría debe estar habilitada](#)

[\[GuardDuty.6\] La protección GuardDuty Lambda debe estar habilitada](#)

[\[GuardDuty.7\] La monitorización del GuardDuty EKS tiempo de ejecución debe estar habilitada](#)

[\[GuardDuty.8\] La protección contra GuardDuty malware para EC2 debe estar habilitada](#)

[\[GuardDuty.9\] La GuardDuty RDS protección debe estar habilitada](#)

[\[GuardDuty.10\] La protección GuardDuty S3 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 ECR escaneo de Amazon Inspector debe estar activado](#)

[\[Inspector.3\] 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 VPC Lambda 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](#)

[\[MSK.1\] MSK Los clústeres deben cifrarse en tránsito entre los nodos intermediarios](#)

[\[MSK.3\] Los conectores MSK Connect deben estar cifrados 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 bases de datos de Neptune deben tener habilitada la autenticación de bases de datos 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 firewalls de Network Firewall \[NetworkFirewall.9\] 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](#)

[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](#)

[\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas 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 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](#)

[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](#)

[\[Redshift.1\] 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](#)

[\[Redshift.7\] Los clústeres de Redshift deberían utilizar un enrutamiento mejorado VPC](#)

[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](#)

[\[S3.1\] 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](#)

[\[S3.5\] Los depósitos de uso general de S3 deberían requerir solicitudes de uso 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 AI notebook no deberían tener acceso directo a Internet](#)

[\[SageMaker.2\] Las instancias de SageMaker AI notebook deben lanzarse en una VPC personalizada](#)

[\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker AI Notebook](#)

[\[SageMaker.4\] Las variantes de producción de terminales de SageMaker IA deben tener un recuento inicial de instancias superior a 1](#)

[\[SageMaker.5\] SageMaker los modelos deberían bloquear el tráfico entrante](#)

[\[SecretsManager.1\] 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 organización de AWS](#)

[\[SNS.4\] las políticas de acceso a los SNS temas no deberían permitir el acceso público](#)

[Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)

[\[SSM.1\] EC2 Las instancias de Amazon deben gestionarse mediante AWS Systems Manager](#)

[\[SSM.2\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche](#)

[\[SSM.3\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)

[\[SSM.4\] SSM los documentos no deben ser públicos](#)

[\[StepFunctions.1\] Las máquinas de estado de Step Functions deberían tener el registro activado](#)

[\[Transfer.2\] Los servidores Transfer Family no deben usar el FTP protocolo para la conexión de puntos finales](#)

[\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)

[\[WAF.2\] Las reglas regionales AWS WAF clásicas deben tener al menos una condición](#)

[\[WAF.3\] Los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla](#)

[\[WAF.4\] La web regional AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

[\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)

[\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)

[\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

[\[WAF.10\] la AWS WAF web ACLs debe tener al menos una regla o grupo de reglas](#)

[\[WAF.12\] AWS WAF las reglas deben tener las CloudWatch métricas habilitadas](#)

[\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)

[\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

Indicador de referencia de CIS AWS Foundations

El Center for Internet Security (CIS) AWS Foundations Benchmark sirve como un conjunto de mejores prácticas de configuración de seguridad. 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 es compatible con CIS AWS Foundations Benchmark v3.0.0, 1.4.0 y v1.2.0.

Esta página enumera los controles de seguridad compatibles con cada versión y proporciona una comparación de las versiones.

AWS CIS Foundations Benchmark v3.0.0

Security Hub es compatible con la versión 3.0.0 del CIS AWS Foundations Benchmark.

Security Hub ha satisfecho los requisitos de la certificación de CIS Security Software, por lo que ha recibido dicha certificación para los siguientes indicadores de referencia de CIS:

- Punto de referencia CIS para CIS AWS Foundations Benchmark, 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 CIS AWS Foundations Benchmark v3.0.0

[\[Account.1\] La información de contacto de seguridad debe proporcionarse para una Cuenta de AWS](#)

[\[CloudTrail.1\] CloudTrail debe habilitarse y configurarse con al menos un registro multirregional que incluya eventos de administración de lectura y escritura](#)

[\[CloudTrail.2\] CloudTrail debe tener activado el cifrado en reposo](#)

[\[CloudTrail.4\] La validación del archivo de CloudTrail registro debe estar habilitada](#)

[\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3](#)

[\[Config.1\] AWS Config debe estar habilitado y usar el rol vinculado al servicio para el registro de recursos](#)

[\[EC2.2\] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente](#)

[\[EC2.6\] El registro de flujo de VPC debe estar habilitado en todas 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 el 0.0.0.0/0 al puerto 22 o al puerto 3389](#)

[\[EC2.53\] los grupos de EC2 seguridad no deberían permitir la entrada desde el 0.0.0.0/0 a los puertos de administración remota del servidor](#)

[\[EC2.54\] Los grupos EC2 de seguridad no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor](#)

[\[EFS.1\] 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](#)

[\[IAM.18\] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte](#)

[\[IAM.22\] 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 la política adjunta 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](#)

[\[S3.5\] Los depósitos de uso general de S3 deberían requerir solicitudes de uso SSL](#)

[\[S3.8\] Los buckets de uso general de S3 deben bloquear el acceso público](#)

[\[S3.20\] Los cubos de uso general de S3 deberían tener habilitada la función de eliminación 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 v1.4.0

Security Hub es compatible con la versión 1.4.0 del CIS AWS Foundations Benchmark.

Controles que se aplican a CIS AWS Foundations Benchmark v1.4.0

[\[CloudTrail.1\] CloudTrail debe habilitarse y configurarse con al menos un registro multirregional que incluya eventos de administración de lectura y escritura](#)

[\[CloudTrail.2\] CloudTrail debe tener activado el cifrado en reposo](#)

[\[CloudTrail.4\] La validación del archivo de CloudTrail registro debe estar habilitada](#)

[\[CloudTrail.5\] CloudTrail Los senderos deben estar integrados con Amazon Logs CloudWatch](#)

[\[CloudTrail.6\] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público](#)

[\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3](#)

[\[CloudWatch.1\] Debe existir un filtro de métrica 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](#)

[\[CloudWatch.5\] Asegúrese de que existan un filtro de métrica de registro y una alarma para los cambios de duración de CloudTrail de AWS Config](#)

[\[CloudWatch.6\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los errores de autenticación de AWS Management Console](#)

[\[CloudWatch.7\] 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 bucket S3](#)

[\[CloudWatch.9\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de configuración de AWS Config](#)

[\[CloudWatch.10\] 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](#)

[\[EC2.2\] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente](#)

[\[EC2.6\] El registro de flujo de VPC debe estar habilitado en todas VPCs](#)

[\[EC2.7\] El cifrado predeterminado de EBS debe estar activado](#)

[\[EC2.21\] La red no ACLs debe permitir la entrada desde el 0.0.0.0/0 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](#)

[\[IAM.18\] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte](#)

[\[IAM.22\] 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](#)

[\[S3.5\] Los depósitos de uso general de S3 deberían requerir solicitudes de uso SSL](#)

[\[S3.8\] Los buckets de uso general de S3 deben bloquear el acceso público](#)

[\[S3.20\] Los cubos de uso general de S3 deberían tener habilitada la función de eliminación MFA](#)

Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0

Security Hub es compatible con la versión 1.2.0 del CIS AWS Foundations Benchmark.

Security Hub ha satisfecho los requisitos de la certificación de CIS Security Software, por lo que ha recibido dicha certificación para los siguientes indicadores de referencia de CIS:

- Punto de referencia CIS para CIS AWS Foundations Benchmark, v1.2.0, nivel 1
- Punto de referencia CIS para CIS AWS Foundations Benchmark, v1.2.0, nivel 2

Controles que se aplican a CIS AWS Foundations Benchmark v1.2.0

[\[CloudTrail.1\] CloudTrail debe habilitarse y configurarse con al menos un registro multirregional que incluya eventos de administración de lectura y escritura](#)

[\[CloudTrail.2\] CloudTrail debe tener activado el cifrado en reposo](#)

[\[CloudTrail.4\] La validación del archivo de CloudTrail registro debe estar habilitada](#)

[\[CloudTrail.5\] CloudTrail Los senderos deben estar integrados con Amazon Logs CloudWatch](#)

[\[CloudTrail.6\] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público](#)

[\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3](#)

[\[CloudWatch.1\] Debe existir un filtro de métrica 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 no autorizadas a la API](#)

[\[CloudWatch.3\] 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](#)

[\[CloudWatch.5\] Asegúrese de que existan un filtro de métrica de registro y una alarma para los cambios de duración de CloudTrail de AWS Config](#)

[\[CloudWatch.6\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los errores de autenticación de AWS Management Console](#)

[\[CloudWatch.7\] 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 bucket S3](#)

[\[CloudWatch.9\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de configuración de AWS Config](#)

[\[CloudWatch.10\] 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](#)

[\[EC2.2\] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente](#)

[\[EC2.6\] El registro de flujo de VPC debe estar habilitado en todas VPCs](#)

[\[EC2.13\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 22](#)

[\[EC2.14\] Los grupos de seguridad no deberían permitir la entrada desde el 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](#)

[\[IAM.18\] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte](#)

[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 v3.0.0, 1.4.0 y 1.2.0 del Indicador de referencia de AWS de Center for Internet Security (CIS).

Security Hub es compatible con cada una de estas versiones del CIS AWS Foundations Benchmark, pero recomendamos usar 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 instrucciones sobre cómo habilitar los estándares, consulte [Habilitación de un estándar de seguridad en Security Hub](#). 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 de Security Hub con varias cuentas AWS Organizations y desea habilitarla por lotes 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
[Account.1] La información de contacto de seguridad debe proporcionarse para una Cuenta de AWS	1.2	1.2	1.18
[CloudTrail.1] CloudTrail debe habilitarse y configurarse con al menos un registro multirregional que incluya eventos de administración de lectura y escritura	3.1	3.1	2.1
[CloudTrail.2] CloudTrail debe tener activado el cifrado en reposo	3.5	3.7	2.7
[CloudTrail.4] La validación del 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] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea 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 CloudTrail bucket de S3			
[CloudWatch.1] Debe existir un filtro de métrica 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 no autorizadas a la API	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] Asegúrese de que existan un filtro de métrica de registro y una alarma para los cambios de duración de CloudTrail de AWS Config	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 autenticación de AWS Management Console	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 bucket 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 configuración de AWS Config	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
[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente	5.4	5.3	4.3
[EC2.6] El registro de flujo de VPC debe estar habilitado en todas 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 deberían permitir la entrada desde el 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 deberían permitir la entrada desde el 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 el 0.0.0.0/0 al puerto 22 o al puerto 3389	5.1	5.1	No compatible
[EC2.53] los grupos de EC2 seguridad no deberían permitir la entrada desde el 0.0.0.0/0 a los puertos de administración remota del servidor	5.2	No admitido	No admitido
[EC2.54] Los grupos EC2 de seguridad no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor	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

ID y título de control	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[IAM.3] Las claves de acceso de los usuarios de IAM deben rotarse cada 90 días o menos	1.14	1.14	1.4
[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

ID y título de control	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[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
[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] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte	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

ID y título de control	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[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
[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 la política adjunta 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

ID y título de control	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[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
[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] Los depósitos de uso general de S3 deberían requerir solicitudes de uso 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

ID y título de control	Requisito del CIS v3.0.0	Requisito del CIS v1.4.0	Requisito del CIS v1.2.0
[S3.20] Los cubos de uso general de S3 deberían tener habilitada la función de eliminación MFA	2.1.2	2.1.3	No compatible: el CIS agregó este requisito en versiones posteriores

ARNs para CIS AWS Foundations Benchmark

Cuando habilite una o más versiones de CIS AWS Foundations Benchmark, empezará 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 de Security Hub para averiguar 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 crea cuando te suscribes a un estándar llamando [BatchEnableStandards](#) en una región.

Note

Al habilitar una versión de CIS AWS Foundations Benchmark, Security Hub puede tardar hasta 18 horas en generar los resultados de 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 más 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 [Ejemplos de resultados de control en Security Hub](#).

Requisitos del CIS que no se admiten en Security Hub

Como se indica en la tabla anterior, Security Hub 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 de forma manual revisando el estado de los recursos de AWS .

NIST SP 800-53 Rev. 5 en Security Hub

El 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 lo ayuda a proteger la disponibilidad, confidencialidad e integridad de sus sistemas de información y recursos críticos. Los organismos del gobierno federal de EE. UU. y los contratistas deben cumplir con la norma NIST SP 800-53 para proteger sus sistemas, pero las empresas privadas pueden utilizarla voluntariamente como marco orientativo para reducir el riesgo de ciberseguridad.

Security Hub proporciona controles que admiten determinados requisitos del NIST SP 800-53. Estos controles se evalúan mediante controles de seguridad automatizados. Los controles de Security Hub no son compatibles con los requisitos del NIST SP 800-53 que requieren comprobaciones manuales. Además, los controles de Security Hub solo admiten los requisitos automatizados del NIST SP 800-53 que aparecen como requisitos relacionados en los detalles de cada control. Seleccione un control de la siguiente lista para ver la información detallada de control. Los requisitos relacionados que no se mencionan en los detalles de control no son compatibles actualmente con Security Hub.

A diferencia de otros marcos, el NIST SP 800-53 no establece prescripciones sobre cómo deben evaluarse sus requisitos. En cambio, el marco proporciona pautas y los controles del Security Hub NIST SP 800-53 representan la comprensión que el servicio tiene de ellas.

Si utiliza la integración de Security Hub AWS Organizations para gestionar de forma centralizada varias cuentas y quiere habilitar por lotes el NIST SP 800-53 en todas ellas, puede ejecutar un [script multicuenta de Security Hub desde la cuenta](#) de administrador.

Para obtener más información sobre el NIST SP 800-53 Rev. 5, consulte el [Centro de recursos de seguridad informática del NIST](#).

Controles aplicables al NIST SP 800-53 Rev. 5

[\[Account.1\] La información de contacto de seguridad debe proporcionarse para una Cuenta de AWS](#)

[\[Account.2\] Cuentas de AWS debe ser parte de una organización de AWS Organizations](#)

[\[ACM.1\] Los certificados importados y ACM emitidos deben renovarse después de un período de tiempo específico](#)

[\[APIGateway.1\] La API puerta de enlace REST y el registro de WebSocket API ejecuciones deben estar habilitados](#)

[\[APIGateway.2\] REST API Las etapas de la API puerta de enlace deben configurarse para usar SSL certificados para la autenticación de fondo](#)

[\[APIGateway.3\] REST API Las etapas de API Gateway deben tener habilitado el AWS X-Ray rastreo](#)

[\[APIGateway.4\] La API puerta de enlace debe estar asociada a una web WAF ACL](#)

[\[APIGateway.5\] Los datos de la REST API caché 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 de API Gateway V2](#)

[\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves API](#)

[\[AutoScaling.1\] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar controles de ELB estado](#)

[\[AutoScaling.2\] 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](#)

[Los puntos de recuperación de \[Backup.1\] AWS Backup deben estar cifrados en reposo](#)

[\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)

[\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)

[\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)

[\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)

[\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)

[\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)

[\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)

[\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)

[\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 multirregional que incluya eventos de administración de lectura y escritura](#)

[\[CloudTrail.2\] CloudTrail debe tener activado el cifrado en reposo](#)

[\[CloudTrail.4\] La validación del archivo de CloudTrail registro debe estar habilitada](#)

[\[CloudTrail.5\] CloudTrail Los senderos deben estar integrados con Amazon Logs CloudWatch](#)

[\[CloudWatch.15\] Las alarmas de CloudWatch deben tener configuradas acciones específicas](#)

[\[CloudWatch.16\] Los grupos de registros de CloudWatch deben retenerse durante un periodo específico](#)

[\[CloudWatch.17\] Las acciones de alarma de CloudWatch 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 estar cifrados en reposo](#)

[\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)

[\[DMS.6\] las instancias de DMS replicación deben tener habilitada la actualización automática de las versiones secundarias](#)

[\[DMS.7\] las tareas de DMS replicación de la base de datos de destino deben tener habilitado el registro](#)

[\[DMS.8\] las tareas de DMS replicación de la base de datos de origen deben tener el registro activado](#)

[\[DMS.9\] Los DMS puntos finales deben utilizar SSL](#)

[\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización IAM](#)

[\[DMS.11\] DMS Los puntos finales de MongoDB deberían tener habilitado un mecanismo de autenticación](#)

[\[DMS.12\] DMS Los puntos finales de Redis deberían estar habilitados OSS TLS](#)

[\[DocumentDB.1\] 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 \(\) deben cifrarse en reposo DAX](#)

[\[DynamoDB.4\] 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 deberían poder restaurarse públicamente](#)

[\[EC2.2\] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente](#)

[\[EC2.3\] Los volúmenes adjuntos de Amazon EBS deben cifrarse en reposo](#)

[\[EC2.4\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)

[\[EC2.6\] El registro de flujo de VPC debe estar habilitado en todas 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 deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 22](#)
- [\[EC2.15\] EC2 Las subredes de Amazon no deberían 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 deberían permitir el tráfico entrante sin restricciones en los puertos autorizados](#)
- [\[EC2.19\] Los grupos de seguridad no deberían permitir el acceso sin restricciones a los puertos de alto riesgo](#)
- [\[EC2.20\] Los dos túneles VPN de una conexión AWS Site-to-Site VPN deben estar activos](#)
- [\[EC2.21\] La red no ACLs debe permitir la entrada desde el 0.0.0.0/0 al puerto 22 o al puerto 3389](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC2.24\] No se deben usar 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 respaldo](#)
- [\[EC2.51\] Los puntos finales de 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 ECR privados deben tener configurado el escaneo de imágenes](#)

[\[ECR.2\] Los repositorios ECR privados deben tener configurada la inmutabilidad de las etiquetas](#)

[\[ECR.3\] ECR Los repositorios deben tener configurada al menos una política de ciclo de vida](#)

[\[ECS.1\] Las definiciones de ECS tareas de Amazon deben tener modos de red seguros y definiciones de usuario.](#)

[\[ECS.2\] ECS los servicios no deberían tener direcciones IP públicas asignadas automáticamente](#)

[\[ECS.3\] las definiciones de ECS tareas no deben compartir el espacio de nombres del proceso del host](#)

[\[ECS.4\] los ECS contenedores deberían ejecutarse sin privilegios](#)

[\[ECS.5\] ECS Los contenedores 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 ECS tareas deben tener una configuración de registro](#)

[\[ECS.10\] Los servicios de ECS Fargate deberían ejecutarse en la última versión de la plataforma Fargate](#)

[\[ECS.12\] ECS los clústeres 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](#)

[\[EFS.2\] EFS Los volúmenes de Amazon deberían estar en los planes de respaldo](#)

[\[EFS.3\] los puntos de EFS acceso deben establecer un directorio raíz](#)

[\[EFS.4\] los puntos de EFS acceso deben imponer la identidad de un usuario](#)

[\[EFS.6\] Los destinos de EFS montaje no deben estar asociados a una subred pública](#)

[\[EKS.1\] Los puntos finales de los EKS clústeres no deben ser de acceso público](#)

[\[EKS.2\] EKS los clústeres deberían ejecutarse en una versión compatible de Kubernetes](#)

[\[EKS.3\] los EKS clústeres deben usar secretos de Kubernetes cifrados](#)

[\[EKS.8\] EKS los clústeres deben tener habilitado el registro de auditoría](#)

[\[ElastiCache.1\] Los clústeres ElastiCache \(RedisOSS\) 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 \(RedisOSS\) de versiones anteriores deberían tener Redis activado OSS AUTH](#)

[\[ElastiCache.7\] 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](#)

[\[ELB.1\] Application Load Balancer debe configurarse para redirigir todas las HTTP solicitudes a HTTPS](#)

[\[ELB.2\] Los balanceadores de carga clásicos con HTTPS listenersSSL/deben usar un certificado proporcionado por AWS Certificate Manager](#)

[\[ELB.3\] Los oyentes de Classic Load Balancer deben configurarse con o con terminación HTTPS TLS](#)

[\[ELB.4\] Application Load Balancer debe configurarse para eliminar los encabezados http no válidos](#)

[\[ELB.5\] El registro de aplicaciones y balanceadores de carga clásicos debe estar habilitado](#)

[\[ELB.6\] Los balanceadores de carga de aplicaciones, puertas de enlace y redes deben tener habilitada la protección contra eliminaciones](#)

[\[ELB.7\] Los balanceadores de carga clásicos deberían tener habilitado el drenaje de conexiones](#)

[\[ELB.8\] Los balanceadores de carga clásicos que utilizan dispositivos de SSL escucha deben usar una política de seguridad predefinida que tenga una larga duración AWS Config](#)

[\[ELB.9\] Los balanceadores de carga clásicos deberían tener activado el balanceo de cargas entre zonas](#)

[\[ELB.10\] Classic Load Balancer debe abarcar varias zonas de disponibilidad](#)

[\[ELB.12\] Application Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)

[\[ELB.13\] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad](#)

[\[ELB.14\] El Classic Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)

[\[ELB.16\] Los balanceadores de carga de aplicaciones deben estar asociados a una web AWS WAF ACL](#)

[\[EMR.1\] 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](#)

[\[FSx.1\] FSx para sistemas de ZFS archivos abiertos, debe configurarse para copiar etiquetas a copias de seguridad y volúmenes](#)

[\[FSx.2\] FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad](#)

[\[GuardDuty.1\] GuardDuty debe 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 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 lambda deben estar en un VPC](#)

[\[Lambda.5\] Las funciones VPC Lambda 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](#)

[\[MSK.1\] MSK Los clústeres deben cifrarse en tránsito entre los nodos intermediarios](#)

[\[MSK.2\] MSK los clústeres deben 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 bases de datos de Neptune deben tener habilitada la autenticación de bases de datos 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](#)

[\[NetworkFirewall.1\] Los 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 firewalls de Network Firewall \[NetworkFirewall.9\] 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](#)

[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 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](#)

[\[RDS.34\] 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](#)

[\[Redshift.1\] 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](#)

[\[Redshift.7\] Los clústeres de Redshift deberían utilizar un enrutamiento mejorado VPC](#)

[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](#)

[\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas 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](#)

[\[S3.5\] Los depósitos de uso general de S3 deberían requerir solicitudes de uso 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 cubos de uso general de S3 deberían tener habilitada la función de eliminación MFA](#)

[\[SageMaker.1\] Las instancias de Amazon SageMaker AI notebook no deberían tener acceso directo a Internet](#)

[\[SageMaker.2\] Las instancias de SageMaker AI notebook deben lanzarse en una VPC personalizada](#)

[\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker AI Notebook](#)

[\[SageMaker.4\] Las variantes de producción de terminales de SageMaker IA 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 organización de AWS](#)

[\[SNS.1\] SNS los temas 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 gestionarse mediante AWS Systems Manager](#)

[\[SSM.2\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche](#)

[\[SSM.3\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)

[\[SSM.4\] SSM los documentos no deben ser públicos](#)

[\[Transfer.2\] Los servidores Transfer Family no deben usar el FTP protocolo para la conexión de puntos finales](#)

[\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)

[\[WAF.2\] Las reglas regionales AWS WAF clásicas deben tener al menos una condición](#)

[\[WAF.3\] Los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla](#)

[\[WAF.4\] La web regional AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

[\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)

[\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)

[\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

[\[WAF.10\] la AWS WAF web ACLs debe tener al menos una regla o grupo de reglas](#)

[\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado](#)

[\[WAF.12\] AWS WAF las reglas deben tener las CloudWatch métricas habilitadas](#)

PCI DSS en Security Hub

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 cuenta con un estándar PCI DSS para ayudarle 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 del PCI SSC validaron este estándar.

Security Hub 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 instrucciones sobre cómo habilitar los estándares, consulte [Habilitación de un estándar de seguridad en Security Hub](#). Si actualmente usa la v3.2.1 pero solo quiere usar la v4.0.1, habilite la versión más reciente antes de deshabilitar la versión anterior. De este modo, se evitan brechas en las comprobaciones de seguridad. Si utiliza la integración de Security Hub con varias cuentas AWS Organizations y desea habilitarla por lotes en varias cuentas, le recomendamos que utilice la [configuración central](#) para hacerlo.

En las siguientes secciones se muestran 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

[\[AutoScaling.1\] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar controles de ELB estado](#)

[\[CloudTrail.2\] CloudTrail debe tener activado el cifrado en reposo](#)

[\[CloudTrail.3\] Debe estar habilitada al menos una CloudTrail ruta](#)

[\[CloudTrail.4\] La validación del 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 métrica 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 deberían poder restaurarse públicamente](#)

[\[EC2.2\] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente](#)

[\[EC2.6\] El registro de flujo de VPC debe estar habilitado en todas VPCs](#)

[\[EC2.12\] Amazon no utilizado EC2 EIPs debería retirarse](#)

[\[EC2.13\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 22](#)

[\[ELB.1\] Application Load Balancer debe configurarse para redirigir todas las HTTP solicitudes 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 debe 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 para los usuarios de IAM deben tener una duración estricta AWS Config](#)

[\[IAM.19\] 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 lambda deben estar en un 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](#)

[\[S3.5\] Los depósitos de uso general de S3 deberían requerir solicitudes de uso SSL](#)

[\[S3.7\] Los buckets de uso general de S3 deben usar la replicación entre regiones](#)

[\[SageMaker.1\] Las instancias de Amazon SageMaker AI notebook no deberían tener acceso directo a Internet](#)

[\[SSM.1\] EC2 Las instancias de Amazon deben gestionarse mediante AWS Systems Manager](#)

[\[SSM.2\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche](#)

[\[SSM.3\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)

Controles que se aplican a PCI DSS v4.0.1

[\[ACM.1\] Los certificados importados y ACM emitidos deben renovarse después de un período de tiempo específico](#)

[\[ACM.2\] RSA los certificados gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)

[\[APIGateway.9\] El registro de acceso debe configurarse para las etapas de API Gateway V2](#)

[\[AppSync.2\] AWS AppSync debe tener activado 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 deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes y los orígenes personalizados](#)

[\[CloudFront.12\] CloudFront las distribuciones no deben apuntar a orígenes S3 inexistentes](#)

[\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)

[\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)

[\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)

[\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)

[\[CloudTrail.2\] CloudTrail debe tener activado el cifrado en reposo](#)

[\[CloudTrail.3\] Debe estar habilitada al menos una CloudTrail ruta](#)

[\[CloudTrail.4\] La validación del archivo de CloudTrail registro debe estar habilitada](#)

[\[CloudTrail.6\] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público](#)

[\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de 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](#)

[\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización IAM](#)

[\[DMS.11\] DMS Los puntos finales de MongoDB deberían tener habilitado un mecanismo de autenticación](#)

[\[DMS.12\] DMS Los puntos finales de Redis deberían estar habilitados OSS TLS](#)

[\[DMS.6\] las instancias de DMS replicación deben tener habilitada la actualización automática de las versiones secundarias](#)

[\[DMS.7\] las tareas de DMS replicación de la base de datos de destino deben tener habilitado el registro](#)

[\[DMS.8\] las tareas de DMS replicación de la base de datos de origen deben tener el registro activado](#)

[\[DMS.9\] Los DMS puntos finales deben utilizar 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 deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 22](#)

[\[EC2.14\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 3389](#)

[\[EC2.15\] EC2 Las subredes de Amazon no deberían 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 utilizar la versión 2 \(\) del Servicio de Metadatos de Instancia IMDSv2](#)

[\[EC2.171\] Las conexiones EC2 VPN deben tener el registro activado](#)

[\[EC2.21\] La red no ACLs debe permitir la entrada desde el 0.0.0.0/0 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](#)

[\[EC2.51\] Los puntos finales de EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)

[\[EC2.53\] los grupos de EC2 seguridad no deberían permitir la entrada desde el 0.0.0.0/0 a los puertos de administración remota del servidor](#)

[\[EC2.54\] Los grupos EC2 de seguridad no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor](#)

[\[EC2.8\] EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancias IMDSv2](#)

[\[ECR.1\] Los repositorios ECR privados deben tener configurado el escaneo de imágenes](#)

[\[ECS.10\] Los servicios de ECS Fargate deberían ejecutarse en la última versión de la plataforma Fargate](#)

[\[ECS.16\] Los conjuntos de ECS tareas no deben asignar automáticamente direcciones IP públicas](#)

[\[ECS.2\] ECS los servicios 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 EFS acceso deben imponer la identidad de un usuario](#)

[\[EKS.1\] Los puntos finales de los EKS clústeres no deben ser de acceso público](#)

[\[EKS.2\] EKS los clústeres deberían ejecutarse en una versión compatible de Kubernetes](#)

[\[EKS.3\] los EKS clústeres deben usar secretos de Kubernetes cifrados](#)

[\[EKS.8\] EKS los clústeres 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 \(RedisOSS\) de versiones anteriores deberían tener Redis activado OSS AUTH](#)

[\[ElasticBeanstalk.2\] Las actualizaciones de la plataforma gestionada de Elastic Beanstalk deben estar habilitadas](#)

[\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)

[\[ELB.12\] Application Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)

[\[ELB.14\] El Classic Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)

[\[ELB.3\] Los oyentes de Classic Load Balancer deben configurarse con o con terminación HTTPS TLS](#)

[\[ELB.4\] Application Load Balancer debe configurarse para eliminar los encabezados http no válidos](#)

[\[ELB.8\] Los balanceadores de carga clásicos que utilizan dispositivos de SSL escucha deben usar una política de seguridad predefinida que tenga una larga duración 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 debe estar activado](#)

[\[GuardDuty.10\] La protección GuardDuty S3 debe estar habilitada](#)

[\[GuardDuty.6\] La protección GuardDuty Lambda debe estar habilitada](#)

[\[GuardDuty.7\] La monitorización del GuardDuty EKS tiempo de ejecución debe estar habilitada](#)

[\[GuardDuty.9\] La GuardDuty RDS protección debe estar habilitada](#)

[\[IAM.10\] Las políticas de contraseñas para los usuarios de IAM deben tener una duración estricta AWS Config](#)

[\[IAM.11\] 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](#)

[\[IAM.18\] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte](#)

[\[IAM.19\] 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 ECR escaneo de Amazon Inspector debe estar activado](#)

[\[Inspector.3\] 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](#)

[\[MSK.1\] MSK Los clústeres deben cifrarse en tránsito entre los nodos intermediarios](#)

[\[MSK.3\] Los conectores MSK Connect deben estar cifrados 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](#)

[\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas 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](#)

[\[S3.5\] Los depósitos de uso general de S3 deberían requerir solicitudes de uso 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 AI 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 de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche](#)

[\[SSM.3\] EC2 Las instancias de Amazon gestionadas 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 Transfer Family no deben usar el FTP protocolo para la conexión de puntos finales](#)

[\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)

[\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado](#)

AWS Estándar de etiquetado de recursos

En esta sección se proporciona información sobre el estándar de etiquetado AWS de recursos.

Note

El estándar AWS de etiquetado de recursos no está disponible en el oeste de Canadá (Calgary), China y las regiones. AWS GovCloud (US)

¿Qué es el estándar de etiquetado AWS de recursos?

Las etiquetas son pares de claves y valores que actúan como metadatos para organizar AWS los recursos. En la mayoría de AWS los recursos, tienes la opción de añadir etiquetas al crear el recurso o después de crearlo. Algunos ejemplos de recursos son una CloudFront distribución de Amazon, una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o una entrada secreta AWS Secrets Manager. Las etiquetas pueden ayudarle a administrar, identificar, organizar, buscar y filtrar 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](#).

El estándar de etiquetado de AWS recursos, desarrollado por AWS Security Hub, le ayuda a determinar si alguno de sus AWS recursos carece de claves de etiqueta. Puede personalizar el `requiredTagKeys` parámetro para especificar las claves de etiquetas que desee que comprueben los controles. Si no se proporcionan etiquetas específicas, los controles solo comprueban la existencia de al menos una clave de etiqueta.

Al activar el estándar de etiquetado de AWS recursos, empezará a recibir los resultados en el formato de búsqueda AWS de seguridad (ASFF).

Note

Al habilitar el estándar de etiquetado de AWS recursos, Security Hub puede tardar hasta 18 horas en generar las conclusiones de los controles que utilizan la misma regla AWS

Config vinculada a servicios que los controles habilitados en otros estándares habilitados. Para obtener más información, consulte [Programación para ejecutar comprobaciones de seguridad](#).

Este estándar 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 de Security Hub para encontrar el ARN de un estándar habilitado.

Controles del estándar de etiquetado AWS de recursos

El estándar AWS de etiquetado de recursos incluye los siguientes controles. Elija un control para revisar una descripción detallada del mismo.

- [\[ACM.3\] ACM los certificados deben estar etiquetados](#)
- [\[AppConfig.1\] 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 de recuperación de AWS Backup deben etiquetarse](#)
- [\[Backup.3\] Los almacenes de AWS Backup deben etiquetarse](#)
- [\[Backup.4\] Los planes de informes de AWS Backup deben etiquetarse](#)
- [\[Backup.5\] Los planes de copias de seguridad de AWS Backup deben etiquetarse](#)
- [\[Batch.1\] 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](#)
- [\[CloudFormation.2\] Las pilas de CloudFormation deben etiquetarse](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CloudTrail.9\] las CloudTrail rutas deben estar etiquetadas](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact 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](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.2\] DMS los certificados deben estar etiquetados](#)
- [\[DMS.3\] las suscripciones a DMS eventos deben estar etiquetadas](#)
- [\[DMS.4\] las instancias de DMS replicación deben estar etiquetadas](#)
- [\[DMS.5\] los grupos de subredes de DMS replicación deben estar etiquetados](#)
- [\[DynamoDB.5\] Las tablas de DynamoDB deben etiquetarse](#)
- [\[EC2.33\] Los archivos adjuntos a las pasarelas de EC2 tránsito deben estar etiquetados](#)
- [\[EC2.34\] Las tablas de rutas de las pasarelas de EC2 tránsito deben estar etiquetadas](#)
- [Las interfaces de EC2 red deben estar etiquetadas \[EC2.35\]](#)
- [\[EC2.36\] Las pasarelas de EC2 clientes deben estar etiquetadas](#)
- [\[EC2.37\] Las direcciones IP EC2 elásticas deben estar etiquetadas](#)
- [\[EC2.38\] EC2 las instancias deben estar etiquetadas](#)
- [\[EC2.39\] Las pasarelas EC2 de Internet deben estar etiquetadas](#)
- [\[EC2.40\] Las pasarelas EC2 NAT deben estar etiquetadas](#)
- [La EC2 red \[EC2.41\] ACLs debe estar etiquetada](#)
- [Las tablas de EC2 rutas deben estar etiquetadas \[EC2.42\]](#)
- [\[EC2.43\] 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 punto final de Amazon VPC deben estar etiquetados](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben estar etiquetados](#)
- [\[EC2.49\] Las conexiones de emparejamiento de Amazon VPC deben estar etiquetadas](#)
- [\[EC2.50\] Las pasarelas de EC2 VPN deben estar etiquetadas](#)
- [\[EC2.52\] Las pasarelas de EC2 tránsito deben estar etiquetadas](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[ECS.13\] ECS los servicios deben estar etiquetados](#)
- [\[ECS.14\] los ECS clústeres deben estar etiquetados](#)
- [\[ECS.15\] Las definiciones de ECS tareas deben estar etiquetadas](#)
- [\[EFS.5\] los puntos de EFS acceso deben estar etiquetados](#)
- [\[EKS.6\] EKS los clústeres deben estar etiquetados](#)
- [\[EKS.7\] Las configuraciones de los proveedores de EKS identidad deben estar etiquetadas](#)
- [\[ES.9\] 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 etiquetarse](#)
- [\[Glue.1\] 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](#)
- [\[IoT.1\] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse](#)
- [\[IoT.2\] Las acciones de mitigación de AWS IoT Core deben etiquetarse](#)
- [\[IoT.3\] Las dimensiones de AWS IoT Core deben etiquetarse](#)

- [\[IoT.4\] Los autorizadores de AWS IoT Core deben etiquetarse](#)
- [\[IoT.5\] Los alias de los roles de AWS IoT Core deben etiquetarse](#)
- [\[IoT.6\] Las políticas de AWS IoT Core deben etiquetarse](#)
- [\[IoTEvents .1\] 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](#)
- [\[IoTtwinmaker.1\] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados](#)
- [\[IoTtwinmaker.2\] Los TwinMaker espacios de trabajo de AWS IoT deben estar etiquetados](#)
- [\[IoTtwinmaker.3\] TwinMaker Las escenas de AWS IoT deben estar etiquetadas](#)
- [\[IoTtwinmaker.4\] 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 IVS deben estar etiquetados](#)
- [\[IVS.2\] Las configuraciones de grabación del IVS deben estar etiquetadas](#)
- [\[IVS.3\] Los canales 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](#)
- [\[NetworkFirewall.7\] Los firewall 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](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 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](#)
- [\[SNS.3\] SNS los temas deben estar etiquetados](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[StepFunctions.2\] Las actividades de Step Functions deben estar etiquetadas](#)
- [\[Transfer.1\] AWS Transfer Family Los flujos de trabajo deben estar etiquetados](#)

Estándares administrados por servicios en Security Hub

Un estándar de administración de servicios es un estándar de seguridad que otro Servicio de AWS administra, pero que se puede ver en Security Hub. Por ejemplo, Estándar gestionado por [servicios: AWS Control Tower es un estándar gestionado](#) por servicios que gestiona. AWS Control Tower Un estándar de administración de servicios difiere de un estándar de seguridad que AWS Security Hub administra 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 de administración de servicios de una de estas formas, el estándar no aparecerá en la consola de Security Hub y no podrá acceder a él mediante la API de Security Hub o AWS CLI.
- Sin activación automática de los controles: al crear un estándar de administración de servicios, Security Hub y el servicio de administración no habilitan automáticamente los controles que se aplican al estándar. Además, cuando Security Hub lanza nuevos controles para el estándar, no

se habilitan automáticamente. Esto se aparta de los estándares que gestiona Security Hub. Para obtener más información sobre la forma habitual de configurar los controles en Security Hub, consulte [Descripción de los controles de seguridad en Security Hub](#).

- **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 los controles existentes del Security Hub o un subconjunto de ellos.

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 los resultados de control, los estados de control y la puntuación de seguridad estándar en la consola de Security Hub, en la API 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 de gestión de servicios: AWS Control Tower](#)

Estándar de gestión de servicios: 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 y AWS Control Tower. Le permite configurar los controles proactivos AWS Control Tower junto con los controles de detección de Security Hub en el AWS Control Tower servicio.

Los controles proactivos ayudan a garantizar el cumplimiento de Cuentas de AWS las 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 de administración de servicios difieren de los estándares que administra AWS Security Hub. Por ejemplo, debe crear y eliminar un estándar administrado por un servicio en el servicio de administración. Para obtener más información, consulte [Estándares administrados por servicios en Security Hub](#).

En la consola y la API de Security Hub, puede ver Service-Managed Standard: AWS Control Tower junto con otros estándares de Security Hub.

Creación del estándar

Este estándar solo está disponible si lo crea en. AWS Control Tower AWS Control Tower crea el estándar al habilitar por primera vez un control aplicable mediante uno de los métodos siguientes:

- AWS Control Tower consola
- AWS Control Tower API (llame a la [EnableControlAPI](#))
- AWS CLI (ejecuta el [enable-control](#) comando)

Los controles del 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, AWS Control Tower también habilita Security Hub por usted.

Si no lo has configurado AWS Control Tower, no podrás ver este estándar ni acceder a él en la consola de Security Hub, en la API 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 sin crear primero 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 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 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](#))

Al cambiar el estado de activación de un control en AWS Control Tower, el cambio también se refleja en Security Hub.

Sin embargo, si se desactiva un control en Security Hub que esté activado, el AWS Control Tower control se desvía. El estado del control se AWS Control Tower muestra como `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 habilitas y deshabilitas los controles en Security Hub (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 utilizar 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 Security Hub, API 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 el estado de activación Disabled en Security Hub, a menos que se habilite explícitamente ese control en Security Hub.

Security Hub 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 [Visualización de los detalles de un control](#).

En función de los estados de control, Security Hub calcula una [puntuación de seguridad](#) para Service-Managed Standard: AWS Control Tower. Esta puntuación solo está disponible en Security Hub. Además, solo puede ver los [resultados de los controles](#) en Security Hub. La puntuación de seguridad estándar y los resultados de control no están disponibles en AWS Control Tower.

Note

Al habilitar los controles para Service-Managed Standard: AWS Control Tower, Security Hub puede tardar hasta 18 horas en generar los resultados de los controles que utilizan una regla vinculada a un AWS Config servicio existente. Es posible que ya tengas reglas vinculadas a servicios si has activado otros estándares y controles en Security Hub. 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 de Security Hub y ya no se puede acceder a él mediante la API de Security Hub o AWS CLI.

 Note

La desactivación de todos los controles del estándar en Security Hub no desactiva ni elimina el estándar.

Al deshabilitar el servicio 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. Security Hub informa de los resultados 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 los resultados de Service-Managed Standard:, consulte. [AWS Control Tower Ejemplos de resultados de control en Security Hub](#)

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 de la siguiente tabla para ver información al respecto, incluidos los pasos para corregir los errores detectados.

La siguiente lista muestra los controles disponibles para el estándar gestionado por el servicio: . 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, si los [resultados de control](#)

[consolidados](#) están desactivados en su cuenta, el campo `ProductFields.ControlId` usa el identificador de control basado en estándares. El ID de control estándar tiene el formato `CT.ControlId`(por ejemplo, `CT.CodeBuild.1`).

- [\[Account.1\] La información de contacto de seguridad debe proporcionarse para una Cuenta de AWS](#)
- [\[ACM.1\] Los certificados importados y ACM emitidos deben renovarse después de un período de tiempo específico](#)
- [\[ACM.2\] RSA los certificados gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)
- [\[APIGateway.1\] La API puerta de enlace REST y el registro de WebSocket API ejecuciones deben estar habilitados](#)
- [\[APIGateway.2\] REST API Las etapas de la API puerta de enlace deben configurarse para usar SSL certificados para la autenticación de fondo](#)
- [\[APIGateway.3\] REST API Las etapas de API Gateway deben tener habilitado el AWS X-Ray rastreo](#)
- [\[APIGateway.4\] La API puerta de enlace debe estar asociada a una web WAF ACL](#)
- [\[APIGateway.5\] Los datos de la REST API caché 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 de API Gateway V2](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves API](#)
- [\[AutoScaling.1\] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar controles de ELB estado](#)
- [\[AutoScaling.2\] 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 multirregional que incluya eventos de administración de lectura y escritura](#)
- [\[CloudTrail.2\] CloudTrail debe tener activado el cifrado en reposo](#)
- [\[CloudTrail.4\] La validación del archivo de CloudTrail registro debe estar habilitada](#)
- [\[CloudTrail.5\] CloudTrail Los senderos deben estar integrados con Amazon Logs CloudWatch](#)
- [\[CloudTrail.6\] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea 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 DMS puntos finales deben utilizar 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 \(\) deben cifrarse en reposo DAX](#)
- [\[EC2.1\] Las instantáneas de Amazon EBS no deberían poder restaurarse públicamente](#)
- [\[EC2.2\] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente](#)
- [\[EC2.3\] Los volúmenes adjuntos de Amazon EBS deben cifrarse en reposo](#)
- [\[EC2.4\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)

- [\[EC2.6\] El registro de flujo de VPC debe estar habilitado en todas 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](#)
- [\[EC2.15\] EC2 Las subredes de Amazon no deberían 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 deberían permitir el tráfico entrante sin restricciones en los puertos autorizados](#)
- [\[EC2.19\] Los grupos de seguridad no deberían permitir el acceso sin restricciones a los puertos de alto riesgo](#)
- [\[EC2.20\] Los dos túneles VPN de una conexión AWS Site-to-Site VPN deben estar activos](#)
- [\[EC2.21\] La red no ACLs debe permitir la entrada desde el 0.0.0.0/0 al puerto 22 o al puerto 3389](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon no utilizados deberían 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 ECR privados deben tener configurado el escaneo de imágenes](#)
- [\[ECR.2\] Los repositorios ECR privados deben tener configurada la inmutabilidad de las etiquetas](#)
- [\[ECR.3\] ECR Los repositorios deben tener configurada al menos una política de ciclo de vida](#)
- [\[ECS.1\] Las definiciones de ECS tareas de Amazon deben tener modos de red seguros y definiciones de usuario.](#)
- [\[ECS.2\] ECS los servicios no deberían tener direcciones IP públicas asignadas automáticamente](#)
- [\[ECS.3\] las definiciones de ECS tareas no deben compartir el espacio de nombres del proceso del host](#)
- [\[ECS.4\] los ECS contenedores deberían ejecutarse sin privilegios](#)

- [\[ECS.5\] ECS Los contenedores 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 de ECS Fargate deberían ejecutarse en la última versión de la plataforma Fargate](#)
- [\[ECS.12\] ECS los clústeres 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](#)
- [\[EFS.2\] EFS Los volúmenes de Amazon deberían estar en los planes de respaldo](#)
- [\[EFS.3\] los puntos de EFS acceso deben establecer un directorio raíz](#)
- [\[EFS.4\] los puntos de EFS acceso deben imponer la identidad de un usuario](#)
- [\[EKS.1\] Los puntos finales de los EKS clústeres no deben ser de acceso público](#)
- [\[EKS.2\] EKS los clústeres deberían ejecutarse en una versión compatible de Kubernetes](#)
- [\[ElastiCache.3\] 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 \(RedisOSS\) de versiones anteriores deberían tener Redis activado OSS AUTH](#)
- [\[ElasticBeanstalk.1\] 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](#)
- [\[ELB.1\] Application Load Balancer debe configurarse para redirigir todas las HTTP solicitudes a HTTPS](#)
- [\[ELB.2\] Los balanceadores de carga clásicos con HTTPS listenersSSL/deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.3\] Los oyentes de Classic Load Balancer deben configurarse con o con terminación HTTPS TLS](#)
- [\[ELB.4\] Application Load Balancer debe configurarse para eliminar los encabezados http no válidos](#)
- [\[ELB.5\] El registro de aplicaciones y balanceadores de carga clásicos debe estar habilitado](#)

- [\[ELB.6\] Los balanceadores de carga de aplicaciones, puertas de enlace y redes deben tener habilitada la protección contra eliminaciones](#)
- [\[ELB.7\] Los balanceadores de carga clásicos deberían tener habilitado el drenaje de conexiones](#)
- [\[ELB.8\] Los balanceadores de carga clásicos que utilizan dispositivos de SSL escucha deben usar una política de seguridad predefinida que tenga una larga duración AWS Config](#)
- [\[ELB.9\] Los balanceadores de carga clásicos deberían tener activado el balanceo de cargas entre zonas](#)
- [\[ELB.10\] Classic Load Balancer debe abarcar varias zonas de disponibilidad](#)
- [\[ELB.12\] Application Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.13\] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad](#)
- [\[ELB.14\] El Classic Load Balancer 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 debe 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 lambda deben estar en un VPC](#)
- [\[Lambda.5\] Las funciones VPC Lambda deben funcionar en varias zonas de disponibilidad](#)
- [\[MSK.1\] MSK Los clústeres 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 bases de datos de Neptune deben tener habilitada la autenticación de bases de datos 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](#)
- [\[Redshift.7\] Los clústeres de Redshift deberían utilizar un enrutamiento mejorado VPC](#)

- [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](#)
- [\[S3.5\] Los depósitos de uso general de S3 deberían requerir solicitudes de uso 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 AI notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] Las instancias de SageMaker AI notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker AI 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 gestionarse mediante AWS Systems Manager](#)

- [\[SSM.2\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche](#)
- [\[SSM.3\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [\[SSM.4\] SSM los documentos no deben ser públicos](#)
- [\[WAF.2\] Las reglas regionales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.3\] Los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.4\] La web regional AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.10\] la AWS WAF web ACLs debe tener al menos una regla o grupo de reglas](#)

Para obtener más información sobre este estándar, consulte los [controles de Security Hub](#) en la Guía del usuario de AWS Control Tower .

Habilitación de un estándar de seguridad en Security Hub

Al activar un estándar de seguridad AWS Security Hub, todos los controles que se aplican al estándar se activan automáticamente en él. Security Hub también comienza a ejecutar controles de seguridad y generar resultados para los controles que se aplican al estándar.

Antes de activar cualquier norma de seguridad, debe activar el registro de recursos AWS Config para todos los recursos que utilizan los controles que se aplican a la norma. De lo contrario, es posible que Security Hub no pueda generar resultados para los controles que se aplican al estándar. Para obtener más información, consulte [Consideraciones antes de habilitar y configurar AWS Config](#).

Puede elegir qué controles desea habilitar y deshabilitar en cada estándar. Al deshabilitar un control, se impide que se generen los resultados del control y el control se ignora al calcular los puntajes de seguridad.

Al activar Security Hub, Security Hub calcula la puntuación de seguridad inicial de un estándar 30 minutos después de su primera visita a la página Resumen o a la página Normas de seguridad de la consola 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) Region. Las puntuaciones solo se generan para los estándares que están activados al visitar esas páginas. Además, el registro AWS Config de recursos debe estar configurado para que aparezcan las puntuaciones. Tras la primera generación de puntuaciones, Security Hub actualiza las puntuaciones de seguridad cada 24 horas. Security Hub muestra una marca de tiempo para indicar cuándo se actualizó por última vez

una puntuación de seguridad. Para ver una lista de los estándares que están actualmente habilitados en su cuenta, invoque la [GetEnabledStandardsAPI](#).

Las instrucciones para habilitar un estándar varían en función de si se utiliza o no la [configuración centralizada](#). Puede utilizar la configuración central si integra Security Hub y AWS Organizations. Recomendamos utilizar la configuración centralizada si desea habilitar los estándares en entornos con varias cuentas y regiones. Si no utiliza la configuración centralizada, debe habilitar cada estándar de forma individual en cada cuenta y región.

Habilitación de un estándar en varias cuentas y regiones

Para habilitar un estándar de seguridad en varias cuentas Regiones de AWS, debe usar la [configuración central](#).

Cuando se utiliza la configuración centralizada, el administrador delegado puede crear políticas de configuración de Security Hub que habiliten uno o varios estándares. A continuación, puedes 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 solo las mejores prácticas de seguridad AWS fundamentales (FSBP) en una unidad organizativa, y puede optar por habilitar FSBP y Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 en otra unidad organizativa. Para obtener instrucciones sobre cómo crear una política de configuración que habilite estándares específicos, consulte [Creación y asociación de políticas de configuración](#)

Si utiliza la configuración centralizada, Security Hub no habilita automáticamente ningún estándar en las cuentas nuevas ni existentes. En cambio, al crear una política de configuración, el administrador delegado define qué estándares se deben habilitar en las diferentes cuentas. Security Hub ofrece una política de configuración recomendada en la que solo está configurado FSBP. Para obtener más información, consulte [Tipos de políticas de configuración](#).

Note

[El administrador delegado puede crear políticas de configuración para habilitar cualquier estándar, excepto el estándar gestionado por servicios: AWS Control Tower](#) Puede habilitar este estándar solo en el servicio. AWS Control Tower Si utiliza la configuración centralizada, puede habilitar y deshabilitar los controles de este estándar para una cuenta administrada centralmente solo en AWS Control Tower.

Si quiere que algunas cuentas configuren sus propios estándares en lugar del administrador delegado, este puede designar esas cuentas como autoadministradas. Las cuentas autoadministradas deben configurar los estándares por separado en cada región.

Habilitación de un estándar 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 estándares en varias cuentas y regiones. Sin embargo, puede seguir estos pasos para habilitar un estándar en una sola cuenta y región.

Security Hub console

Habilitación de un estándar en una cuenta y región

1. Abra la AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>.
2. Confirme que está utilizando Security Hub en la región en la que desea deshabilitar el estándar.
3. En el panel de navegación de Security Hub, elija Estándares de seguridad.
4. Para el estándar que desea habilitar, elija Enable (Habilitar). Esto también habilita todos los controles dentro de ese estándar.
5. Repítalo en cada región en la que quiera habilitar el estándar.

Security Hub API

Habilitación de un estándar en una cuenta y región

1. Invoca el [BatchEnableStandardsAPI](#).
2. Proporcione el nombre de recurso de Amazon (ARN) del estándar que quiera habilitar. Para obtener el ARN estándar, invoque la [DescribeStandardsAPI](#).
3. Repítalo en cada región en la que quiera habilitar el estándar.

AWS CLI

Habilitación de un estándar en una cuenta y región

1. Ejecute la [batch-enable-standardscomando](#)

- Proporcione el nombre de recurso de Amazon (ARN) del estándar que quiera habilitar. Para obtener el ARN estándar, ejecute el [describe-standardscomando](#)

```
aws securityhub batch-enable-standards --standards-subscription-requests  
'{"StandardsArn": "standard ARN"}'
```

Ejemplo

```
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"}'
```

- Repítalo en cada región en la que quiera habilitar el estándar.

Desactivación de un estándar de seguridad en Security Hub

Cuando deshabilita un estándar de seguridad en Security Hub, ocurre lo siguiente:

- Todos los controles que se aplican a la norma también están desactivados, a menos que estén asociados a otra norma.
- Las comprobaciones para los controles deshabilitados ya no se realizan y no se generan resultados adicionales para los controles deshabilitados.
- Los resultados existentes sobre los controles deshabilitados se archivan automáticamente después de un plazo aproximado de 3 a 5 días.
- Se eliminan las AWS Config reglas que Security Hub creó para los controles deshabilitados.

Esto suele ocurrir unos minutos después de desactivar el estándar, pero puede tardar más. Si se produce un error en la primera solicitud para eliminar AWS Config las reglas, Security Hub lo vuelve a intentar cada 12 horas. Sin embargo, si deshabilitó Security Hub o no tiene ningún otro estándar habilitado, Security Hub no podrá volver a intentar la solicitud, lo que significa que no podrá eliminar las reglas de AWS Config. Si esto ocurre y necesita eliminar AWS Config las reglas, póngase en contacto con Soporte.

Desactivación de un estándar en varias cuentas y regiones

Para deshabilitar un estándar de seguridad en varias cuentas y regiones, debe utilizar la [configuración centralizada](#).

Cuando utiliza la configuración centralizada, el administrador delegado puede crear políticas de configuración que deshabiliten uno o varios estándares. Puede asociar una política de configuración a cuentas 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 deshabilitar el Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS) en una unidad organizativa y deshabilitar tanto el PCI DSS como el SP 800-53 Rev. 5 del Instituto Nacional de Estándares y Tecnología (NIST) en otra unidad organizativa. Para obtener instrucciones sobre cómo crear una política de configuración que deshabilite estándares específicos, consulte [Creación y asociación de políticas de configuración](#).

Note

El administrador delegado puede crear políticas de configuración para deshabilitar cualquier estándar, excepto el estándar [gestionado por servicios](#). AWS Control Tower Puede deshabilitar este estándar solo en el servicio. AWS Control Tower Si utiliza la configuración centralizada, puede habilitar y deshabilitar los controles de este estándar para una cuenta administrada centralmente solo en AWS Control Tower.

Si quiere que algunas cuentas configuren sus propios estándares en lugar del administrador delegado, este puede designar esas cuentas como autoadministradas. Las cuentas autoadministradas deben configurar los estándares por separado en cada región.

Deshabilitación de un estándar en una sola cuenta y región

Si no utiliza la configuración central o tiene una cuenta autoadministrada, no podrá utilizar las políticas de configuración para deshabilitar de manera centralizada los estándares en varias cuentas y regiones. Sin embargo, puede seguir estos pasos para deshabilitar un estándar en una sola cuenta y región.

Security Hub console

Deshabilitación de un estándar en una cuenta y región

1. Abra la AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>.
2. Confirme que está utilizando Security Hub en la región en la que desea deshabilitar el estándar.

3. En el panel de navegación de Security Hub, elija Estándares de seguridad.
4. Para el estándar que desea deshabilitar, elija Disable (Deshabilitar).
5. Repítalo en cada región en la que quiera deshabilitar el estándar.

Security Hub API

Deshabilitación de un estándar en una cuenta y región

1. Invoca el [BatchDisableStandardsAPI](#).
2. Para cada estándar que desee deshabilitar, proporcione el ARN de la suscripción estándar. Para obtener la suscripción ARNs para sus estándares habilitados, invoque la [GetEnabledStandardsAPI](#).
3. Repítalo en cada región en la que quiera deshabilitar el estándar.

AWS CLI

Deshabilitación de un estándar en una cuenta y región

1. Ejecute la [batch-disable-standardscomando](#)
2. Para cada estándar que desee deshabilitar, proporcione el ARN de la suscripción estándar. Para obtener la suscripción ARNs para los estándares habilitados, ejecute la [get-enabled-standardscomando](#)

```
aws securityhub batch-disable-standards --standards-subscription-arns "standard  
subscription ARN"
```

Ejemplo

```
aws securityhub batch-disable-standards --standards-subscription-arns  
"arn:aws:securityhub:us-west-1:123456789012:subscription/aws-foundational-  
security-best-practices/v/1.0.0"
```

3. Repítalo en cada región en la que quiera deshabilitar el estándar.

Desactivar los estándares activados automáticamente

Si no utiliza la configuración centralizada, su organización utiliza un tipo de configuración denominado configuración local. Con la configuración centralizada, Security Hub puede habilitar automáticamente los estándares de seguridad predeterminados en las cuentas de miembro nuevas cuando se unen a su organización. Todos los controles que forman parte de los estándares predeterminados también se habilitan automáticamente.

Actualmente, los estándares de seguridad predeterminados que se activan automáticamente son AWS Foundational Security Best Practices v1.0.0 y Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Puede desactivar los estándares que se habilitan automáticamente si prefiere habilitarlos manualmente en cuentas nuevas.

Si utiliza la configuración centralizada, puede crear una política de configuración que habilite los estándares predeterminados y asociar esta política a la raíz. Todas las cuentas de su organización OUs heredarán esta política de configuración, a menos que estén asociadas a una política diferente o sean autogestionadas.

Los siguientes pasos solo se aplican si se integra con la configuración local AWS Organizations y la utiliza. Si no utiliza la integración con Organizations, puede desactivar un estándar predeterminado la primera vez que habilite Security Hub o puede seguir los pasos para [Deshabilitación de un estándar en una sola cuenta y región](#).

Security Hub console

Para desactivar de forma automática de los estándares habilitados (consola)

1. Abra la AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>.
Inicie sesión en las credenciales de una cuenta del administrador.
2. En el panel de navegación de Security Hub, en Configuración, elija Configuración.
3. En la sección Cuentas, desactive la opción Habilitar automáticamente los estándares predeterminados.

Security Hub API

Para desactivar de forma automática de los estándares habilitados (API)

Utilizar [UpdateOrganizationConfiguration](#) funcionamiento de la API de Security Hub desde la cuenta de administrador de Security Hub. Si usa el AWS CLI, ejecute el [update-organization-configuration](#) comando

Para desactivar los estándares habilitados automáticamente de las cuentas de los miembros nuevos, establezca el valor de `AutoEnableStandards` como igual a `NONE`.

Por ejemplo, el siguiente AWS CLI comando desactiva los estándares activados automáticamente. 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-organization-configuration --auto-enable-standards NONE
```

Visualización de los detalles de un estándar

En la AWS Security Hub consola, la página de detalles de un estándar incluye la siguiente información:

- La puntuación de seguridad del estándar
- Resumen visual de los estados de control que se aplican al estándar.
- El resumen visual de los controles de seguridad de los controles que están habilitados en el estándar. Si se integra con AWS Organizations, los controles que están habilitados en al menos una cuenta de la organización se consideran habilitados.
- Una lista de los controles que se aplican a la norma. Puede filtrar y ordenar los controles según sea necesario.

En esta sección se explica cómo recuperar los detalles de un estándar.

Para ver los detalles de un estándar (consola)

1. Abra la AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>.
2. En el panel de navegación de Security Hub, elija Estándares de seguridad.
3. Para el estándar para el que desea mostrar los detalles, elija Ver resultados.

Descripción de la puntuación de seguridad del estándar

En la parte superior de la página de detalles estándar se encuentra la puntuación de seguridad del estándar. La puntuación es el porcentaje de controles aprobados en relación con el número de controles habilitados (que tienen datos) para el estándar.

Por lo general, Security Hub calcula la puntuación de seguridad inicial 30 minutos después de la primera visita a la página Resumen o a la página Normas de seguridad de la consola de Security Hub. Las puntuaciones solo se generan para los estándares que están activados al visitar esas páginas. Para ver una lista de los estándares que están habilitados actualmente, utilice la operación de API [GetEnabledStandards](#). Además, se debe configurar el registro de recursos de AWS Config para que aparezcan las puntuaciones. Tras la primera generación de puntuaciones, Security Hub actualiza las puntuaciones de seguridad cada 24 horas. Security Hub muestra una marca de tiempo para indicar cuándo se actualizó por última vez una puntuación de seguridad. Para obtener más información sobre cómo se calculan las puntuaciones, consulte [the section called “Calcular las puntuaciones de seguridad”](#).

Note

Las puntuaciones de seguridad por primera vez pueden tardar hasta 24 horas en generarse en las regiones de China y de AWS GovCloud (US) Region.

Junto a la puntuación hay un gráfico que resume los controles de seguridad de los controles que están habilitados en el estándar. El gráfico muestra la cantidad de controles de seguridad aprobados y no aprobados. También puede elegir un nivel de gravedad específico para ver los controles de seguridad no aprobados para los controles del nivel de gravedad elegido

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.

Todos los datos de las páginas de detalles de las Normas de seguridad son específicos de la región actual, a menos que haya establecido una región de agregación. Si ha establecido una región de agregación, las puntuaciones de seguridad se aplican a todas las regiones e incluyen los resultados de todas las regiones vinculadas. El estado de cumplimiento de los controles en las páginas de detalles de las normas también refleja los resultados de las regiones vinculadas, y el número de controles de seguridad incluye los resultados de las regiones vinculadas.

Visualización de los controles de un estándar habilitado

Al visitar la página de detalles de un estándar, puede ver una lista de los controles de seguridad que se aplican al estándar.

Para cada control, la tabla muestra la siguiente información:

- El identificador y el título del control
- El estado del control. Para obtener más información, consulte [Evaluación del estado de control y el estado de conformidad en Security Hub](#).
- La gravedad asociada con el control
- El número de controles fallidos del número total de controles. Si corresponde, en la columna Comprobaciones con errores también se muestra el número de resultados con el estado Desconocido.
- Si el control admite [parámetros personalizados](#).

Security Hub actualiza los estados de control y el recuento de controles de seguridad cada 24 horas. Una marca de tiempo en la parte superior de la página indica cuándo se actualizaron por última vez los estados de control y el recuento de controles de seguridad. Para obtener más información, consulte [the section called “Estado de conformidad y el estado de control”](#).

En el caso de las cuentas de administrador, los estados de control y el número de controles de seguridad se agregan a la cuenta de administrador y a todas las cuentas de los miembros. El recuento de los controles habilitados incluye los controles que están habilitados en el estándar en la cuenta del administrador o al menos en una cuenta de miembro. El recuento de controles deshabilitados incluye los controles que están deshabilitados en el estándar en la cuenta de administrador y en todas las cuentas de los miembros.

De forma predeterminada, la tabla muestra todos los controles habilitados en el estándar. Los controles con un estado de control fallido se muestran en la parte superior, ordenados de forma decreciente según su gravedad.

Puede filtrar la lista de todos los controles del estándar. Con la opción Filtrar situada junto a la tabla, puede elegir ver solo los controles habilitados o deshabilitados en el estándar. Si solo ve los controles habilitados, puede filtrar aún más la lista por estado de control. Esto permite que se centre en los controles con un estado de control específico.

Además de la opción Filtrar, puede ordenar las listas de controles introduciendo los filtros en el cuadro de búsqueda Filtrar controles. Por ejemplo, puede filtrar por ID o título de control.

Elija el método de acceso que prefiera y siga los pasos para mostrar los controles disponibles para un estándar habilitado.

Security Hub console

Cómo ver los controles de un estándar habilitado (consola)

1. Abra la AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>.
2. Elija Estándares de seguridad en el panel de navegación.
3. Seleccione Ver resultados para ver un estándar. En la parte inferior de la página se enumeran todos los controles que se aplican al estándar. Filtre y ordene la lista según sea necesario.

Security Hub API

Para ver los controles de un estándar habilitado (API)

1. Utilizar [ListSecurityControlDefinitions](#) funcionamiento de la API de Security Hub. Si usa el AWS CLI, ejecute el [list-security-control-definitions](#) comando.

Proporcione el nombre de recurso de Amazon (ARN) del estándar del que quiera ver los controles. Para obtener el estándar ARNs, utilice la [DescribeStandards](#) operación o el comando [describe-standards](#). Si no proporciona un ARN estándar, Security Hub devuelve todo el control de seguridad. IDs

2. Utilizar [ListStandardsControlAssociations](#) funcionamiento de la API de Security Hub o del [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. 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 list-standards-control-associations --region us-east-1 --security-control-id Config.1
```

Puede descargar la página actual de la lista de controles a un archivo .csv seleccionando [Descargar](#).

Si filtra la lista de controles, el archivo descargado incluye solo los controles que coinciden con la configuración del filtro.

Descripción de los controles de seguridad en Security Hub

Un control de seguridad es una protección dentro de un estándar de seguridad que ayuda a una organización a proteger la confidencialidad, la integridad y la disponibilidad de su información. En Security Hub, un control está relacionado con un recurso de AWS específico.

Cuando habilita un control en uno o más estándares, Security Hub comienza a ejecutar controles de seguridad en él. Los controles de seguridad dan lugar a los resultados de Security Hub. Cuando deshabilita un control, Security Hub deja de ejecutar los controles de seguridad en él y ya no se generan los resultados correspondientes.

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 centralizada, el administrador delegado de Security Hub puede crear políticas que especifican cómo se debe configurar un control en varias cuentas y regiones. Para obtener más información sobre cómo habilitar y deshabilitar controles, consulte [Habilitación de controles en Security Hub](#).

Vista de controles consolidados

La página Controles de la consola de Security Hub muestra todos los controles disponibles en la Región de AWS actual (puede ver los controles en el contexto de un estándar visitando la página Estándares de seguridad y seleccionando un estándar activado). Security Hub asigna a los controles un identificador, un título y una descripción de control de seguridad coherentes en todos los estándares. Los identificadores de los controles incluyen el Servicio de AWS relevante y un número único (por ejemplo, CodeBuild.3).

La siguiente información está disponible en la página Controles de la [consola 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 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 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 sus Cuenta de AWS y Región de AWS actuales. 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](#).

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 consolidada provoca cambios en los campos de resultado de controles en Formato de resultados de seguridad de AWS (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. Este permiso no es necesario para ver las puntuaciones de seguridad según estándares específicos.

Al activar Security Hub, Security Hub calcula la puntuación de seguridad inicial 30 minutos después de su primera visita a la página Resumen o a la página Normas de seguridad de la consola 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) Region.

Además de la puntuación de seguridad general, Security Hub calcula una puntuación de seguridad para cada estándar activado unos 30 minutos después de su primera visita a la página Resumen o a la página Estándares 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 puntuaciones. Para obtener más información sobre cómo Security Hub calcula las puntuaciones de seguridad, consulte [Calcular las puntuaciones de seguridad](#).

Tras la primera generación de puntuaciones, Security Hub actualiza las puntuaciones de seguridad cada 24 horas. Security Hub 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 controles de Security Hub

Esta referencia de controles proporciona una lista de AWS Security Hub los controles 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 en uso activo por Security Hub. 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 Servicio de AWS e indica el recurso al que se refiere el control. La consola 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, los hallazgos de Security Hub hacen referencia al control de seguridad IDs solo si los hallazgos de control consolidado están activados 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. Si bien Security Hub puede actualizar ocasionalmente los títulos o descripciones de los controles, el control IDs sigue 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. Seleccione un control para ver 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 Security Hub muestra los títulos de los controles de seguridad, independientemente de si los resultados de control consolidados están activados o desactivados en su cuenta. Sin embargo, los resultados de Security Hub hacen referencia a los títulos de control de seguridad solo si los resultados de control consolidado están activados 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 del control específico del estándar con el control IDs de seguridad IDs, consulte [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 Security Hub determina la gravedad del control, consulte [Nivel 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. Seleccione un control para ver los detalles de los parámetros. Para obtener más información, consulte [Descripción de los parámetros de control en Security Hub](#).

Seleccione un control para ver sus detalles. Los controles se muestran en orden alfabético según el nombre del servicio.

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	MEDIO		N Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
		de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower			
Account.2	Cuenta de AWS debería ser parte de una AWS Organizations organización	NIST SP 800-53 Rev. 5	ALTO		N 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, 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		N El cambio se ha activado
ACM.3	Los certificados ACM 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
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
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, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	MEDIO	N	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	N	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
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		NEI El cambio se ha activado
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		NEI 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

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
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	N	El cambio se ha activado
AppConfig1.	AWS AppConfig las aplicaciones deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
AppConfig2.	AWS AppConfig los perfiles de configuración deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
AppConfig3.	AWS AppConfig los entornos deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
AppConfig4.	AWS AppConfig las asociaciones de extensiones 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
AppFlow1.	AppFlow Los flujos de Amazon deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
AppRunner1.	Los servicios de App Runner deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
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 fundamentales de seguridad, versión 1.0.0	MEDIO	N	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

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
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	¡N	El cambio se ha activado
AppSync6.	AWS AppSync Las cachés de las API deben estar cifradas en tránsito	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0	MEDIO	N	El cambio se ha activado
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 v1.0.0	MEDIO	N	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
AutoScaling1.	Los grupos de escalado automático o asociados con un equilibrador de carga deben usar comprobaciones de estado de ELB	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	BAJA		N El cambio se ha activado
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		N El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Autoscaling.5	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		NEI El cambio se ha activado
AutoScaling6.	Los grupos de escalado automático 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		NEI 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. 5 AWS Control Tower 5	MEDIO		NEI El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
AutoScaling.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	Sí	El cambio se ha activado
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

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Lote.1	AWS Batch las colas de trabajos deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Lote.2	AWS Batch las políticas de programación deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Lote 3	AWS Batch los entornos de cómputo deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Lote.1	AWS Batch las colas de trabajos deben estar etiquetadas	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		N El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
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		N El cambio se ha activado
CloudFront4.	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		Y El cambio se ha activado
CloudFront5.	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		N El cambio se ha activado
CloudFront6.	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		N El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudFront7.	CloudFront las distribuciones deben usar certificados SSL/TLS personalizados	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 Rev. 5	MEDIO		El cambio se ha activado
CloudFront8.	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		El cambio se ha activado
CloudFront9.	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		El cambio se ha activado
CloudFront10.	CloudFront las distribuciones no deben usar protocolos SSL obsoletos entre las ubicaciones de borde y los orígenes personalizados	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO		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.t.12	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		N Periódico
CloudFront.t.13	CloudFront las distribuciones deben usar el control de acceso al origen	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO		N El cambio se ha activado
CloudFront.t.14	CloudFront las distribuciones deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
CloudTrail.1.	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, AWS Foundational Security Best Practices v1.0.0, estándar de gestión de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	ALTO		N 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 Foundations Benchmark v1.4.0 AWS 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	MEDIO		N Periódico
CloudTrail I3.	Debe estar habilitado al menos un CloudTrail sendero	PCI DSS v3.2.1, PCI DSS v4.0.1	ALTO		N 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 v1.2.0, AWS Foundational Security Best Practices v1.0.0, estándar de gestión de servicios: PCI DSS v3.2.1, PCI DSS v4.0.1 AWS Control Tower, CIS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5 AWS	BAJA		N 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		N Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudTrail 16.	Asegúrese de que el depósito de S3 utilizado 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		N El cambio se desencadena y es periódico
CloudTrail 17.	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		N Periódico
CloudTrail 19.	CloudTrail los senderos deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
CloudWatch 1.	Debe existir un filtro de métrica de registro y una alarma para el uso del usuario raíz	CIS AWS Foundations Benchmark v1.2.0, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS	BAJA		N Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudWatch h2.	Asegurar que haya un filtro de métricas de registro y alarma para las llamadas a la API no autorizadas	Punto de referencia sobre AWS los fundamentos de la CEI v1.2.0	BAJA		N 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		N 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 v1.2.0, CIS AWS Foundations Benchmark v1.4.0	BAJA		N Periódico
CloudWatch h5.	Asegúrese de que existan un registro métrico, un filtro y una alarma para los cambios CloudTrail de configuración	CIS AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0	BAJA		N Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
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 v1.2.0, CIS AWS Foundations Benchmark v1.4.0	BAJA		N 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 v1.2.0, CIS AWS Foundations Benchmark v1.4.0	BAJA		N 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 v1.2.0, CIS AWS Foundations Benchmark v1.4.0	BAJA		N Periódico
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 v1.2.0, CIS AWS Foundations Benchmark v1.4.0	BAJA		N Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudWatch h.10	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios de grupos de seguridad	Índice de referencia sobre AWS fundaciones de la CEI versión 1.2.0, punto de referencia sobre las bases de la CEI AWS versión 1.4.0	BAJA		N Periódico
CloudWatch h.11	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)	Índice de referencia de AWS fundamentos de la CEI versión 1.2.0, punto de referencia de fundamentos de la CEI AWS versión 1.4.0	BAJA		N Periódico
CloudWatch h.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 AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0	BAJA		N Periódico
CloudWatch h.13	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en la tabla de enrutamiento	Índice de referencia sobre AWS fundaciones de la CEI versión 1.2.0, punto de referencia sobre las bases de la CEI AWS versión 1.4.0	BAJA		N Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
CloudWatch h.14	Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en la VPC	Índice de referencia sobre AWS fundaciones de la CEI versión 1.2.0, punto de referencia sobre las bases de la CEI AWS versión 1.4.0	BAJA		N Periódico
CloudWatch h.15	CloudWatch las alarmas deben tener configuradas las acciones especificadas	NIST SP 800-53 Rev. 5	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 h.17	CloudWatch las acciones de alarma deben estar habilitadas	NIST SP 800-53 Rev. 5	ALTO		N El cambio se ha activado
CodeArtifact1.	CodeArtifact los repositorios 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
CodeBuild 1.	CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales	AWS Prácticas recomendadas de seguridad fundamentales 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	CRÍTICO		N El cambio se ha activado
CodeBuild 2.	CodeBuild las variables de entorno del proyecto no deben contener credenciales de texto claro	AWS Prácticas recomendadas de seguridad fundamentales 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	CRÍTICO		N El cambio se ha activado
CodeBuild 3.	CodeBuild Los registros de S3 deben estar cifrados	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios:, AWS Control Tower	BAJA		N 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 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		N El cambio se ha activado
CodeBuild 7.	CodeBuild las exportaciones de los grupos de informes deben estar cifradas en reposo	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO		N 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
CodeGuruReviewer1.	CodeGuru Las asociaciones de repositorios de Reviewer 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
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 Prácticas recomendadas de seguridad fundamentales, versión 1.0.0	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 v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1	CRÍTICO	Sí	Periódico
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

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
DataFirehose1.	Los flujos de entrega de Firehose deben estar cifrados en reposo	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO		Periódico
DataSync1.	DataSync las tareas deberían tener el registro activado	AWS Mejores prácticas fundamentales de seguridad, versión 1.0.0	MEDIO		El cambio se ha activado
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 Prácticas recomendadas de seguridad fundamentales 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	CRÍTICO		Periódico
DMS.2	Los certificados DMS 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
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
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 v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO		N 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 Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO		N 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.8	Las tareas de replicación del DMS para la base de datos de origen deben tener el registro habilitado	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO		NEI cambio se ha activado
DMS.9	Los puntos finales del DMS deben usar SSL	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO		NEI cambio se ha activado
DMS.10	Los puntos de conexión de DMS para las bases de datos de Neptune deben tener habilitada la autorización de IAM	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO		NEI cambio se ha activado
DMS.11	Los puntos de conexión de DMS para MongoDB deben tener un mecanismo de autenticación habilitado	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO		NEI cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
DMS.12	Los puntos de conexión de DMS para Redis OSS deben tener el TLS habilitado	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO		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		El cambio se ha activado
DocumentB.2	Los clústeres de Amazon DocumentDB deben tener un período de retención de copias de seguridad adecuado	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, 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
DocumentDB B.3	Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, NIST SP 800-53 rev. 5, PCI DSS v4.0.1	CRÍTICO	No	El cambio se ha activado
DocumentDB B.4	Los clústeres de Amazon DocumentDB deben publicar los registros de auditoría en Logs CloudWatch	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
DocumentDB 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	¡Sí!	El cambio se ha activado
DynamoDB 1	Las tablas de DynamoDB deberían escalar automáticamente la capacidad en función de la demanda	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, 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
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		N El cambio se ha activado
DynamoDB 3	Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO		¡ El cambio se ha activado Periódico
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		¡ El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
DynamoDB 7	Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO		N Periódico
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 AWS Control Tower, NIST SP 800-53 rev. 5	CRÍTICO		N 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		N 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.	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 Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 rev. 5 AWS	MEDIO	N	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	N	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 v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO	S	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	N	El cambio se ha activado
EC2.10	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 administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	N	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.12	Los que no se usen EC2 EIPs deben ser retirados	PCI DSS v3.2.1, NIST SP 800-53 rev. 5	BAJA		N El cambio se ha activado
EC2.13	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	ALTO		N El cambio se desencadena y es periódico
EC2.14	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		N El cambio se desencadena y es periódico
EC2.15	EC2 las subredes no deberían asignar automáticamente direcciones IP públicas	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios:, AWS Control Tower	MEDIO		N El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.16	Deben eliminarse las listas de control de acceso a la red no utilizadas	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios:, AWS Control Tower	BAJA		El cambio se ha activado
EC2.17	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		El cambio se ha activado
EC2.18	Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados	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	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 Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	CRÍTICO		N El cambio se desencadena y es periódico
EC2.20	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	MEDIO		N El cambio se ha activado
EC2.21	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, AWS Foundational Security Best Practices v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5, PCI DSS v4.0.1 AWS Control Tower	MEDIO		N El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.22	Se deben eliminar los grupos de seguridad no utilizados	Estándar gestionado por el servicio: AWS Control Tower	MEDIO		N Periódico
EC2.23	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		¡ El cambio se ha activado
EC2.24	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		¡ El cambio se ha activado
EC2.25	EC2 las plantillas de lanzamiento no deben asignar interfaces públicas IPs a las de red	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO		N El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.28	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
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

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
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
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

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
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
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

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC25.0	EC2 Las pasarelas VPN deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
EC25.1	EC2 Los puntos finales de Client VPN deben tener habilitado el registro de conexiones de clientes	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 rev. 5, PCI DSS, versión 4.0.1	BAJA	N	El cambio se ha activado
EC2.52	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	N	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.54	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		N Periódico
EC2.55	VPCs debe configurarse con un punto final de interfaz para la API ECR	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 Rev. 5	MEDIO	Sí	Periódico
EC25.6	VPCs debe configurarse con un punto final de interfaz para Docker Registry	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 Rev. 5	MEDIO	Sí	Periódico
EC25.7	VPCs debe configurarse con un punto final de interfaz para Systems Manager	AWS Prácticas recomendadas fundamentales de seguridad, versión 1.0.0, 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
EC25.8	VPCs debe configurarse con un punto final de interfaz para los contactos de Systems Manager Incident Manager	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, 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 Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 Rev. 5	MEDIO	Sí	Periódico
EC21.70	EC2 las plantillas de lanzamiento deben usar Instance Metadata Service, versión 2 () IMDSv2	AWS Mejores prácticas fundamentales de seguridad v1.0.0, PCI DSS v4.0.1	BAJA		NEI El cambio se ha activado
EC2.171	EC2 Las conexiones VPN deberían tener el registro activado	AWS Mejores prácticas fundamentales de seguridad v1.0.0, PCI DSS v4.0.1	MEDIO		NEI El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EC2.172	EC2 La configuración de acceso público del bloque de VPC debería bloquear el tráfico de las puertas de enlace de Internet	AWS Mejores prácticas fundamentales de seguridad, versión 1.0.0	MEDIO	Sí	El cambio se ha activado
ECR.1	Los repositorios privados de ECR deben tener configurado el escaneo de imágenes	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO		N 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. AWS Control Tower 5	MEDIO		N 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.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. AWS Control Tower 5	MEDIO		N El cambio se ha activado
ECR.4	Los repositorios públicos de ECR deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	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: AWS Control Tower NIST SP 800-53 Rev. 5	ALTO		N 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.2	Los servicios de ECS no deberían tener direcciones IP públicas asignadas automáticamente	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO		NEI cambio se ha activado
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. AWS Control Tower 5	ALTO		NEI 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. AWS Control Tower 5	ALTO		NEI cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
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. AWS Control Tower 5	ALTO		N El cambio se ha activado
ECS.8	Los secretos no deben pasarse como variables de entorno del contenedor	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO		N 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		¡N 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.10	Los servicios Fargate de ECS deberían ejecutarse en la última versión de la plataforma Fargate	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO		El cambio se ha activado
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. AWS Control Tower 5	MEDIO		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

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
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 v1.0.0, PCI DSS v4.0.1	ALTO	N	El cambio se ha activado
EFS.1	Elastic File System 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	N	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. AWS Control Tower 5	MEDIO	N	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. AWS Control Tower 5	MEDIO		N El cambio se ha activado
EFS.4	Los puntos de acceso EFS deben imponer una identidad de usuario	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO		N 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 v1.0.0	MEDIO		N 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 de seguridad fundamentales v1.0.0	MEDIO		N El cambio se ha activado
EFS.8	Los sistemas de archivos de EFS deben cifrarse en reposo	AWS Mejores prácticas de seguridad fundamentales v1.0.0	MEDIO	Sí	El cambio se ha activado
EKS.1	Los puntos de conexión del clúster EKS no deben ser de acceso público	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO		N Periódico
EKS.2	Los clústeres de EKS deben ejecutarse en una versión compatible de Kubernetes	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO		N 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 v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO		N 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 v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO		N 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 fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	ALTO		N 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		N 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		N Periódico
ElastiCache5.	ElastiCache los grupos de replicación deberían ser encrypted-in-transit	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, NIST SP 800-53 rev. 5, PCI DSS v4.0.1	MEDIO		N 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 v1.0.0, NIST SP 800-53 rev. 5, PCI DSS v4.0.1	MEDIO		N 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		N Periódico
ElasticBeanstalk1.	Los entornos de Elastic Beanstalk deberían tener habilitados los informes de estado mejorados	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	BAJA		N 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 v1.0.0, 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 v1.0.0, 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: PCI DSS v3.2.1, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO		N Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
ELB.2	Los equilibradores de carga clásicos con agentes de escucha SSL/HTTPS deben usar un certificado proporcionado por AWS Certificate Manager	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	MEDIO		N El cambio se ha activado
ELB.3	Los oyentes de Equilibrador de carga clásico deben configurarse con una terminación HTTPS o TLS	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO		N El cambio se ha activado
ELB.4	Equilibrador de carga de aplicación debe configurarse para eliminar los encabezados http	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO		N 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. AWS Control Tower 5	MEDIO		N 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 Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	MEDIO		N El cambio se ha activado
ELB.7	Los equilibradores de carga clásicos deberían tener habilitado el drenaje de conexiones	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	MEDIO		N 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 v1.0.0, 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.9	Los equilibradores de carga clásicos deben tener habilitado el equilibrador de carga entre zonas	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	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. 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
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 v1.0.0, NIST SP 800-53 rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO		NEI 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. AWS Control Tower 5	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 v1.0.0, NIST SP 800-53 rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO		NEI 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 AWS web WAF	NIST SP 800-53 Rev. 5	MEDIO		N El cambio se ha activado
EMR.1	Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO		N Periódico
EMR.2	La configuración de bloqueo del acceso público de Amazon EMR debe estar habilitada	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	CRÍTICO		N Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
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 AWS Control Tower, NIST SP 800-53 rev. 5	MEDIO		N Periódico
ES.2	Los dominios de Elasticsearch no deben ser de acceso público	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, 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		N Periódico
ES.3	Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios:, AWS Control Tower	MEDIO		N 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.4	Debe estar habilitado el registro de errores del dominio de Elasticsearch en CloudWatch Logs	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		N El cambio se ha activado
ES.5	Los dominios de Elasticsearch deben tener habilitado el registro de auditoría	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, estándar de administración de servicios: AWS Control Tower	MEDIO		N El cambio se ha activado
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. AWS Control Tower 5	MEDIO		N 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.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. AWS Control Tower 5	MEDIO		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 v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO		El cambio se ha activado
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

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
EventBridge3.	EventBridge los autobuses personalizados para eventos deberían tener adjunta una política basada en los recursos	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, NIST SP 800-53 rev. 5, PCI DSS v4.0.1	BAJA		NI 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		NI 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
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

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
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		N Periódico
FSx2.	FSx para Lustre, los sistemas de archivos deben configurarse para copiar etiquetas a las copias de seguridad	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 Rev. 5	BAJA		N Periódico
Glue.1	AWS Glue los trabajos deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Glue.3	AWS Glue Las transformaciones de aprendizaje automático deben cifrarse en reposo	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0	MEDIO		N El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
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 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	ALTO	N	Periódico
GuardDuty2.	GuardDuty los filtros deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
GuardDuty3.	GuardDuty IPSets debe estar etiquetado	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
GuardDuty4.	GuardDuty los detectores 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
GuardDuty 5.	GuardDuty La supervisión del registro de auditoría de EKS debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad, versión 1.0.0	ALTO	N	Periódico
GuardDuty 6.	GuardDuty La protección Lambda debe estar habilitada	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, PCI DSS v4.0.1	ALTO	N	Periódico
GuardDuty 7.	GuardDuty La monitorización del tiempo de ejecución de EKS debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad v1.0.0, PCI DSS v4.0.1	MEDIO	N	Periódico
GuardDuty 8.	GuardDuty La protección contra malware para EC2 debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad, versión 1.0.0	ALTO	N	Periódico
GuardDuty 9.	GuardDuty La protección RDS debe estar habilitada	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, PCI DSS v4.0.1	ALTO	N	Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
GuardDuty.10	GuardDuty La protección S3 debe estar habilitada	AWS Mejores prácticas fundamentales de seguridad v1.0.0, PCI DSS v4.0.1	ALTO		N Periódico
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, Service Managed Standard: PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	ALTO		N 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, AWS Foundational Security Best Practices v1.0.0, estándar de administración de servicios: PCI DSS v3.2.1, NIST SP 800-53 rev. AWS Control Tower 5	BAJA		N 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 Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO	S	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 Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, estándar de gestión de servicios: PCI DSS v3.2.1, NIST SP 800-53 rev. 5 AWS Control Tower	CRÍTICO	N	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 Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO		S 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 Foundations Benchmark v1.2.0, 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	CRÍTICO		N 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 Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, 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, 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	MEDIO		S Periódico
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		S Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.10	Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras	PCI DSS v3.2.1, PCI DSS v4.0.1	MEDIO		N Periódico
IAM.11	Asegurar que la política de contraseñas de IAM requiere al menos una letra mayúscula	CIS AWS Foundations Benchmark v1.2.0, PCI DSS v4.0.1	MEDIO		N Periódico
IAM.12	Asegurar que la política de contraseñas de IAM requiere al menos una letra minúscula	CIS AWS Foundations Benchmark v1.2.0, PCI DSS v4.0.1	MEDIO		N Periódico
IAM.13	Asegurar que la política de contraseñas de IAM requiere al menos un símbolo	CIS AWS Foundations Benchmark v1.2.0, PCI DSS v4.0.1	MEDIO		N Periódico
IAM.14	Asegurar que la política de contraseñas de IAM requiere al menos un número	CIS AWS Foundations Benchmark v1.2.0, PCI DSS v4.0.1	MEDIO		N Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
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 AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0 AWS	MEDIO		N Periódico
IAM.16	Asegurar que la política de contraseñas de IAM impide la reutilización de contraseñas	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, PCI AWS DSS v4.0.1	BAJA		N Periódico
IAM.17	Asegurar que la política de contraseñas de IAM haga caducar las contraseñas al cabo de 90 días o menos	CIS AWS Foundations Benchmark v1.2.0, PCI DSS v4.0.1	BAJA		N Periódico
IAM.18	Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, CIS Foundations Benchmark v1.2.0, PCI AWS DSS v4.0.1	BAJA		N Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IAM.19	MFA se debe habilitar para todos los usuarios de IAM	NIST SP 800-53 rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	MEDIO		N Periódico
IAM.21	Las políticas de IAM administrada por los clientes que usted cree no deberían permitir acciones comodín para los servicios	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	BAJA		N El cambio se ha activado
IAM.22	Deben eliminarse las credenciales de usuario de IAM que no se hayan utilizado durante 45 días	Índice de referencia de AWS fundaciones de la CEI versión 3.0.0, punto de referencia de AWS fundaciones de la CEI versión 1.4.0	MEDIO		N 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	Los certificados SSL/TLS caducados administrados en IAM deben eliminarse	CIS AWS Foundations Benchmark v3.0.0	MEDIO		N Periódico
IAM.27	Las identidades de IAM no deberían tener la AWSCloudShellFullAccess política adjunta	CIS AWS Foundations Benchmark v3.0.0	MEDIO		N El cambio se ha activado
IAM.28	El analizador de acceso externo del Analizador de acceso de IAM debe estar habilitado	CIS AWS Foundations Benchmark v3.0.0	ALTO		N Periódico
Inspector.1	El EC2 escaneo de Amazon Inspector debe estar activado	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, PCI DSS v4.0.1	ALTO		N Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Inspector .2	El análisis de ECR en Amazon Inspector debe estar habilitado	AWS Mejores prácticas de seguridad fundamentales v1.0.0, PCI DSS v4.0.1	ALTO		N Periódico
Inspector .3	El análisis de código de Lambda en Amazon Inspector debe estar habilitado	AWS Mejores prácticas de seguridad fundamentales v1.0.0, PCI DSS v4.0.1	ALTO		N Periódico
Inspector .4	El análisis de estándar de Lambda en Amazon Inspector debe estar habilitado	AWS Mejores prácticas de seguridad fundamentales v1.0.0, PCI DSS v4.0.1	ALTO		N 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

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IoT.4	AWS IoT Core los autorizadores deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
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

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
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
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

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
IoMaker.2TTwin	AWS TwinMaker Los espacios de trabajo de IoT deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoMaker.3TTwin	AWS TwinMaker Las escenas de IoT deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoMakerTTwin.4	AWS TwinMaker Las entidades de IoT deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoWireless.1.1	AWS Los grupos de multidifusión de IoT Wireless deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoWireless.1.2	AWS Los perfiles de servicio de IoT Wireless deben estar etiquetados	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
IoWireless.1.3	AWS Las tareas de IoT Wireless FUOTA 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
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
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	N	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.2	Las transmisiones de Kinesis deben estar etiquetadas	AWS Estándar de etiquetado de recursos	BAJA	Sí	El cambio se ha activado
Kinesis.3	Las transmisiones de Kinesis deben tener un periodo adecuado de retención de datos	AWS Mejores prácticas fundamentales de seguridad v1.0.0	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: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO		N 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. AWS Control Tower 5	MEDIO		N 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 suprimirse 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		N 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		S Periódico
KMS.5	Las claves KMS no deben ser de acceso público	AWS Mejores prácticas de seguridad fundamentales v1.0.0	CRÍTICO		N 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 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	CRÍTICO		N El cambio se ha activado
Lambda.2	Las funciones de Lambda deben usar los últimos tiempos de ejecución	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO		N 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		N 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. AWS Control Tower 5	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		N 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		N 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 v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO		N El cambio se ha activado
MSK.2	Los clústeres de MSK deberían tener configurada una supervisión mejorada	NIST SP 800-53 Rev. 5	BAJA		N El cambio se ha activado
MSK.3	Los conectores de MSK Connect deben cifrarse en tránsito	AWS Mejores prácticas de seguridad fundamentales v1.0.0, 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 Prácticas recomendadas fundamentales de seguridad v1.0.0, NIST SP 800-53 rev. 5, PCI DSS v4.0.1	MEDIO		N El cambio se ha activado
MQ.3	Los agentes de Amazon MQ deben tener habilitada la actualización automática de las versiones secundarias	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	BAJA		N 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 deben usar el modo de implementación activo/en espera	NIST SP 800-53 Rev. 5, estándar de administración de servicios: AWS Control Tower	BAJA		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		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		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 v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO		NEI 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 v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	CRÍTICO		NEI 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		NEI 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	N	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	N	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		N 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		N 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		N El cambio se ha activado
NetworkFirewall2.	El registro de Network Firewall debe estar habilitado	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5	MEDIO		N 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, versión 1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	MEDIO		N 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		N 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, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	MEDIO		N 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, versión 1.0.0, estándar de administración de servicios: AWS Control Tower NIST SP 800-53 Rev. 5	MEDIO		El cambio se ha activado
NetworkFirewall7.	Los firewalls 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		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 habilitado el cifrado 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		NEI 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		NEI 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		NEI 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 CloudWatch los registros 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		N El cambio se ha activado
Opensearch h.5	OpenSearch los dominios deben tener habilitado el registro de auditoría	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO		N 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		N 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		N El cambio se ha activado
Opensearch h.8	Las conexiones a OpenSearch los dominios deben cifrarse con la política de seguridad TLS más reciente	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		N 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 fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	BAJA		N 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		N Periódico
PCA.1	AWS Private CA la autoridad emisora de certificados raíz debe estar deshabilitada	AWS Prácticas recomendadas fundamentales de seguridad, versión 1.0.0, NIST SP 800-53 Rev. 5	BAJA		N 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		N 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 de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible	CIS AWS Foundations Benchmark v3.0.0, AWS Foundations Security Best Practices v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5, PCI DSS v3.2.1 AWS Control Tower, PCI DSS v4.0.1	CRÍTICO		N 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 AWS Foundations Benchmark v1.4.0, AWS Foundations Security Best Practices v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO		N 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. AWS Control Tower 5	MEDIO		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. AWS Control Tower 5	MEDIO		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. AWS Control Tower 5	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, versión 1.0.0, NIST SP 800-53 Rev. 5	BAJA		N 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 v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	BAJA		N El cambio se ha activado
RDS.9	Las instancias de base de datos de RDS deben publicar los registros en Logs CloudWatch	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO		N 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 v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	MEDIO		NEI 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. AWS Control Tower 5	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, versión 1.0.0, NIST SP 800-53 Rev. 5	MEDIO		NEI 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, AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO		S El cambio se ha activado
RDS.14	Los clústeres de Amazon Aurora deben tener habilitada la característica de búsqueda de datos anteriores	AWS Mejores prácticas fundamentales de seguridad v1.0.0, 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		N 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		N 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 v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	BAJA		N El cambio se ha activado
RDS.18	Las instancias de RDS deben implementarse en una VPC	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	ALTO		N 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 v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	BAJA		N 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 v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	BAJA		NEI 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 v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	BAJA		NEI 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 v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	BAJA		NEI 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 v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	BAJA		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 Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO		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 v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO		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 v1.0.0, NIST SP 800-53 rev. 5, PCI DSS v4.0.1	MEDIO		N 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 Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO		N 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 v1.0.0, 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 Prácticas recomendadas fundamentales de seguridad v1.0.0, PCI DSS v4.0.1	MEDIO		N El cambio se ha activado
RDS.38	Las instancias de base de datos de RDS para PostgreSQL deben cifrarse en tránsito	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0	MEDIO		N Periódico
RDS.39	Las instancias de base de datos de RDS para MySQL deben cifrarse en tránsito	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0	MEDIO		N Periódico
Redshift.1	Los clústeres de Amazon Redshift deberían prohibir el acceso público	AWS Prácticas recomendadas de seguridad fundamentales 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	CRÍTICO		N 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 Prácticas recomendadas de seguridad fundamentales v1.0.0, 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 v1.0.0, 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 v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	MEDIO		NEI 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. AWS Control Tower 5	MEDIO		NEI 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. AWS Control Tower 5	MEDIO		NEI 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. AWS Control Tower 5	MEDIO		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. AWS Control Tower 5	MEDIO		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 v1.0.0, PCI DSS v4.0.1	ALTO		N 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		N El cambio se ha activado
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

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
Route53.2	Las zonas alojadas públicas de Route 53 deben registrar las consultas de DNS	AWS Mejores prácticas fundamentales de seguridad v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO		N El cambio se ha activado
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 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	MEDIO		N Periódico
S3.2	Los buckets de uso general de S3 deben bloquear el acceso público de lectura	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		N 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
S3.3	Los buckets de uso general de S3 deben bloquear el acceso público de escritura	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	N	El cambio se desencadena y es periódico
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 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	MEDIO	N	El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
S3.6	Las políticas de compartimentos de uso general de S3 deberían restringir el acceso a otras Cuentas de AWS	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		N 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		N El cambio se ha activado
S3.8	Los buckets de uso general de S3 deben bloquear el acceso público	CIS AWS Foundations Benchmark v3.0.0, CIS AWS Foundations Benchmark v1.4.0, AWS Foundational Security Best Practices v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	ALTO		S El cambio se ha activado

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
S3.9	Los buckets de uso general de S3 deben tener habilitado el registro de acceso al servidor	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO		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		El cambio se ha activado
S3.11	Los buckets de uso general de S3 deben tener habilitadas las notificaciones de eventos	NIST SP 800-53 Rev. 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
S3.12	ACLs no debe usarse para administrar el acceso de los usuarios a los depósitos de uso general de S3	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		N El cambio se ha activado
S3.13	Los buckets de uso general de S3 deben tener configuraciones de ciclo de vida	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	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	BAJA		N 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, PCI DSS v4.0.1, estándar de administración de servicios: AWS Control Tower	MEDIO		N 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 de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	CRÍTICO		N 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 AWS Foundations Benchmark v1.4.0, NIST SP 800-53 rev. 5	BAJA		N El cambio se ha activado
S3.22	Los buckets de uso general de S3 deben registrar eventos de escritura a nivel de objeto	CIS AWS Foundations Benchmark v3.0.0, PCI DSS v4.0.1	MEDIO		N Periódico
S3.23	Los buckets de uso general de S3 deben registrar eventos de lectura a nivel de objeto	CIS AWS Foundations Benchmark v3.0.0, PCI DSS v4.0.1	MEDIO		N Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
S3.24	Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público	AWS Mejores prácticas de seguridad fundamentales v1.0.0, PCI DSS v4.0.1	ALTO		N El cambio se ha activado
SageMaker 1.	Las instancias de Amazon SageMaker AI Notebook no deberían tener acceso directo a Internet	AWS Prácticas recomendadas de seguridad fundamentales 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	ALTO		N Periódico
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		N 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 3.	Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook	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		N 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 Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 rev. 5	MEDIO		N Periódico
SageMaker 5.	SageMaker los modelos deberían bloquear el tráfico entrante	AWS Mejores prácticas fundamentales de seguridad v1.0.0	MEDIO		N El cambio se ha activado
SecretsManager1.	Los secretos de Secrets Manager deberían tener habilitada la rotación automática	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, 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 v1.0.0, 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 Prácticas recomendadas de seguridad fundamentales v1.0.0, NIST SP 800-53 Rev. 5, estándar de administración 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 v1.0.0, 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 Prácticas recomendadas de seguridad fundamentales, versión 1.0.0, NIST SP 800-53 Rev. 5	ALTO		N 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	MEDIO		N 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 v1.0.0	ALTO		El cambio se ha activado
SQS.1	Las colas de Amazon SQS deben cifrarse en reposo	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	MEDIO		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
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		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.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 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	ALTO		N El cambio se ha activado
SSM.3	EC2 las instancias administradas por Systems Manager deben tener un estado de asociación de COMPLIANT	AWS Prácticas recomendadas de seguridad fundamentales 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		N El cambio se ha activado
SSM.4	Los documentos del SSM no deben ser públicos	AWS Prácticas recomendadas de seguridad fundamentales v1.0.0, estándar de administración de servicios: NIST SP 800-53 Rev. AWS Control Tower 5	CRÍTICO		N Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
StepFunctions1.	Step Functions indica que las máquinas deberían tener el registro activado	AWS Mejores prácticas de seguridad fundamentales v1.0.0, 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
Transfer.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 v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	MEDIO		N Periódico
WAF.1	AWS El registro WAF Classic Global Web ACL debe estar habilitado	AWS Prácticas recomendadas fundamentales de seguridad v1.0.0, NIST SP 800-53 rev. 5, PCI DSS v4.0.1	MEDIO		N Periódico

ID de control de seguridad	Título de control de seguridad	Estándares aplicables	Gravedad	Admite parámetros personalizados	Tipo de programación
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		N El cambio se ha activado
WAF.3	AWS Los grupos de reglas regionales clásicas de la 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		N El cambio se ha activado
WAF.4	AWS La web WAF Classic Regional 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		N 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.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		N 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		N 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		N El cambio se ha activado
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		N 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.11	AWS El registro de ACL web en WAF debe estar habilitado	NIST SP 800-53 rev. 5, PCI DSS v4.0.1	BAJA		N Periódico
WAF.12	AWS Las reglas WAF deben tener las CloudWatch métricas habilitadas	AWS Prácticas recomendadas fundamentales de seguridad, versión 1.0.0, NIST SP 800-53 Rev. 5	MEDIO		N El cambio se ha activado
Workspace s1.	WorkSpaces los volúmenes de usuarios deben cifrarse en reposo	AWS Prácticas recomendadas de seguridad fundamentales, versión 1.0.0	MEDIO		N El cambio se ha activado
Workspace s2.	WorkSpaces los volúmenes raíz deben cifrarse en reposo	AWS Mejores prácticas fundamentales de seguridad, versión 1.0.0	MEDIO		N El cambio se ha activado

Temas

- [Controles de Security Hub para Cuentas de AWS](#)
- [Controles de Security Hub para API Gateway](#)
- [Controles de Security Hub para AWS AppConfig](#)
- [Controles de Security Hub para Amazon AppFlow](#)
- [Controles de Security Hub para AWS App Runner](#)
- [Controles de Security Hub para AWS AppSync](#)
- [Controles de Security Hub para Athena](#)

- [Controles de Security Hub para AWS Backup](#)
- [Controles de Security Hub para AWS Batch](#)
- [Controles de Security Hub para ACM](#)
- [Controles de Security Hub para AWS CloudFormation](#)
- [Controles de Security Hub para CloudFront](#)
- [Controles de Security Hub para CloudTrail](#)
- [Controles de Security Hub para CloudWatch](#)
- [Controles de Security Hub para CodeArtifact](#)
- [Controles de Security Hub para CodeBuild](#)
- [Controles de Security Hub para Amazon CodGuru Profiler](#)
- [Controles de Security Hub para Amazon CodeGuru Reviewer](#)
- [Controles de Security Hub para Amazon Cognito](#)
- [Controles de Security Hub para AWS Config](#)
- [Controles de Security Hub para Amazon Connect](#)
- [Controles de Security Hub para Amazon Data Firehose](#)
- [Controles de Security Hub para DataSync](#)
- [Controles de Security Hub para Detective](#)
- [Controles de Security Hub para AWS DMS](#)
- [Controles de Security Hub para Amazon DocumentDB](#)
- [Controles de Security Hub para DynamoDB](#)
- [Controles de Security Hub para Amazon EC2](#)
- [Controles de Security Hub para el escalado automático](#)
- [Controles de Security Hub para Amazon ECR](#)
- [Controles de Security Hub para Amazon ECS](#)
- [Controles de Security Hub para Amazon EFS](#)
- [Controles de Security Hub para Amazon EKS](#)
- [Controles de Security Hub para ElastiCache](#)
- [Controles de Security Hub para Elastic Beanstalk](#)
- [Controles de Security Hub para equilibradores de carga elásticos](#)
- [Security Hub para Elasticsearch](#)

- [Controles de Security Hub en Amazon EMR](#)
- [Controles de Security Hub para EventBridge](#)
- [Controles de Security Hub para Amazon Fraud Detector](#)
- [Controles de Security Hub para Amazon FSx](#)
- [Controles de Security Hub para Global Accelerator](#)
- [Controles de Security Hub para AWS Glue](#)
- [Controles de Security Hub para GuardDuty](#)
- [Controles de Security Hub para IAM](#)
- [Controles de Security Hub para Amazon Inspector](#)
- [Controles de Security Hub para AWS IoT](#)
- [Controles de Security Hub para eventos de AWS IoT](#)
- [Controles de Security Hub para AWS IoT SiteWise](#)
- [Controles de Security Hub para AWS IoT TwinMaker](#)
- [Controles de Security Hub para AWS IoT Wireless](#)
- [Controles de Security Hub para Amazon IVS](#)
- [Controles de Security Hub para Amazon Keyspaces](#)
- [Controles de Security Hub para Kinesis](#)
- [Controles de Security Hub para AWS KMS](#)
- [Controles de Security Hub para Lambda](#)
- [Controles de Security Hub para Macie](#)
- [Controles de Security Hub para Amazon MSK](#)
- [Controles de Security Hub para Amazon MQ](#)
- [Controles de Security Hub para Neptune](#)
- [Controles de Security Hub para Network Firewall](#)
- [Controles de Security Hub para el OpenSearch servicio](#)
- [Controles de Security Hub para AWS Private CA](#)
- [Controles de Security Hub para Amazon RDS](#)
- [Controles de Security Hub para Amazon Redshift](#)
- [Controles de Security Hub para Route 53](#)
- [Controles de Security Hub para Amazon S3](#)

- [Controles de Security Hub para SageMaker IA](#)
- [Controles de Security Hub para Secrets Manager](#)
- [Controles de Security Hub para Service Catalog](#)
- [Controles de Security Hub para Amazon SES](#)
- [Controles de Security Hub para Amazon SNS](#)
- [Controles de Security Hub para Amazon SQS](#)
- [Controles de Security Hub para Step Functions](#)
- [Controles de Security Hub para Systems Manager](#)
- [Controles de Security Hub para Transfer Family](#)
- [Controles de Security Hub para AWS WAF](#)
- [Controles de Security Hub para WorkSpaces](#)

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 todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[Account.1] La información de contacto de seguridad debe proporcionarse para una 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 permiten a AWS contactar con otra persona si surgen problemas con la cuenta si usted no está disponible. Las notificaciones pueden ser de Soporte u otros equipos de Servicio de AWS acerca de temas relacionados con la seguridad que estén asociados al uso de su Cuenta de AWS.

Corrección

Para agregar un contacto alternativo como contacto de seguridad a su Cuenta de AWS, consulte [Actualizar los contactos alternativos para la Cuenta de AWS](#) en la Guía de referencia de Administración de cuentas de AWS.

[Account.2] Cuentas de AWS debe ser parte de una organización de 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 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 en 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 los recursos y las regiones de Servicios de AWS.

Corrección

Para crear una nueva organización y añadir automáticamente Cuentas de AWS, consulte [Creación de una organización](#) en la Guía del usuario de AWS Organizations. Para añadir cuentas a una organización existente, consulte [Invitar a una Cuenta de AWS a unirse a su organización](#) en la Guía del usuario de AWS Organizations.

Controles de Security Hub para API Gateway

Estos controles de Security Hub evalúan el servicio y los recursos de Amazon API Gateway.

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](#).

[APIGateway.1] La API puerta de enlace REST y el registro de WebSocket API ejecuciones deben estar habilitados

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 un Amazon API Gateway REST o WebSocket API tienen habilitado el registro. El control falla si no lo loggingLevel está ERROR o si INFO ocurre en todas las etapas delAPI. 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.

API La puerta de enlace REST o WebSocket API las etapas deben tener habilitados los registros relevantes. API El registro de WebSocket API ejecución REST y puerta de enlace proporciona registros detallados de las solicitudes realizadas a API Gateway REST y WebSocket API las etapas. Las etapas incluyen las respuestas del backend de la API integración, las respuestas del autorizador Lambda y las de los puntos finales de requestId la AWS integración.

Corrección

Para habilitar el registro REST y WebSocket API las operaciones, consulte [Configurar el CloudWatch API registro mediante la consola API Gateway en la Guía para desarrolladores de Gateway](#). API

[APIGateway.2] REST API Las etapas de la API puerta de enlace deben configurarse para usar SSL certificados para la autenticación de fondo

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 (3), 3, NIST.800-53.r5 SC-1 3, 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 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::ApiGateway::Stage

Regla de AWS Config : [api-gw-ssl-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si REST API las etapas de Amazon API Gateway tienen SSL certificados configurados. Los sistemas de backend utilizan estos certificados para autenticar que las solicitudes entrantes provienen de API Gateway.

API REST API Las etapas de Gateway deben configurarse con SSL certificados para permitir que los sistemas de backend autenticen que las solicitudes se originan en Gateway. API

Corrección

Para obtener instrucciones detalladas sobre cómo generar y configurar los REST API SSL certificados de API Gateway, consulte [Generar y configurar un SSL certificado para la autenticación de backend en la Guía para desarrolladores de APIGateway](#).

[APIGateway.3] REST API Las etapas de API Gateway deben tener habilitado el AWS X-Ray 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 AWS X-Ray activo está habilitado para REST API las etapas 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 del API. El rastreo activo de X-Ray proporciona métricas en tiempo real de las solicitudes de los usuarios que fluyen a través de REST API las operaciones de API Gateway y los servicios conectados.

Corrección

Para obtener instrucciones detalladas sobre cómo habilitar el rastreo activo de X-Ray para REST API las operaciones de API Gateway, consulte la [compatibilidad con el rastreo activo de Amazon API Gateway AWS X-Ray en la Guía para AWS X-Ray](#) desarrolladores.

[APIGateway.4] La API puerta de enlace debe estar asociada a una web WAF ACL

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 puerta de enlace utiliza una lista de control de acceso a la AWS WAF web (ACL). Este control falla si una AWS WAF web no ACL está conectada a una etapa de REST API puerta de enlace.

AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones web contra APIs los ataques. Le permite configurar un ACL, que es un conjunto de reglas que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que la etapa de API Gateway esté asociada a una AWS WAF web ACL para protegerla de ataques malintencionados.

Corrección

Para obtener información sobre cómo usar la consola de API Gateway para asociar una web AWS WAF ACL regional a una API etapa de API Gateway existente, consulte [Uso AWS WAF para protegerla APIs](#) en la Guía para desarrolladores de API Gateway.

[APIGateway.5] Los datos de la REST API caché 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 REST API etapas de API Gateway que tienen la caché habilitada están cifrados. El control falla si algún método de una REST API etapa 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 API permisos para descifrar los datos antes de que puedan leerse.

APIRESTAPI Las cachés de las pasarelas de enlace deben cifrarse en reposo para ofrecer un nivel de seguridad adicional.

Corrección

Para configurar el almacenamiento en API caché de 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: .800-53.r5 NIST CM-2 NIST.800-53.r5 AC-3, .800-53.r5 CM-2 (2) NIST

Categoría: Proteger > Administración de acceso seguro

Gravedad: media

Tipo de recurso: AWS::ApiGatewayV2::Route

AWS Config regla: [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 API rutas	Enum	AWS_IAM, CUSTOM, JWT	Sin valor predeterminado

Este control comprueba si las rutas de Amazon API Gateway tienen un tipo de autorización. El control falla 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`.

APIGateway admite varios mecanismos para controlar y administrar el acceso a su API. Al especificar un tipo de autorización, puede restringir el acceso únicamente API a sus usuarios o procesos autorizados.

Corrección

Para configurar un tipo de autorización HTTP APIs, consulte [Control y administración del acceso a un servidor de API Gateway HTTP API en](#) la Guía para desarrolladores de API Gateway. Para configurar un tipo de autorización WebSocket APIs, consulte [Control y administración del acceso a un servidor de API Gateway WebSocket API en](#) la Guía para desarrolladores de API Gateway.

[APIGateway.9] El registro de acceso debe configurarse para las etapas de API Gateway V2

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), v4.0.1/10.4.2 PCI DSS

Categoría: Identificar - Registro

Gravedad: media

Tipo de recurso: AWS::ApiGatewayV2::Stage

AWS Config regla: [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.

API Los registros de acceso a la pasarela proporcionan información detallada sobre quién ha accedido a su puerta API y cómo ha accedido la persona que ha llamado a ella. API Estos registros son útiles para aplicaciones como auditorías de seguridad y acceso y para investigaciones forenses. Habilite estos registros de acceso para analizar los patrones de tráfico y solucionar problemas.

Para obtener más información sobre las mejores prácticas, consulte la [supervisión REST APIs](#) en la Guía para desarrolladores de API Gateway.

Corrección

Para configurar el registro de acceso, consulte [Configurar el CloudWatch API registro 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	Lista de etiquetas que cumplen los requisitos de AWS	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	Lista de etiquetas que cumplen los requisitos de AWS	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	Lista de etiquetas que cumplen los	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.		requisitos de AWS	

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	Lista de etiquetas que cumplen los requisitos de AWS	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
<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	Lista de etiquetas que cumplen los requisitos de AWS	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 controles de Security Hub evalúan el AWS App Runner 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](#).

[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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un servicio de AWS App Runner 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 añadir etiquetas a un servicio de App Runner, consulta [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-service-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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un conector de VPC de AWS App Runner 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 agregar etiquetas a un conector de VPC de App Runner, 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 todas las Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[AppSync.1] las AWS AppSync API cachés 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 una AWS AppSync API caché está cifrada en reposo. El control falla si la API caché 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 activado el registro a nivel de campo

Requisitos relacionados: v4.0.1/10.4.2 PCI DSS

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
<code>fieldLoggingLevel</code>	Nivel de registro del campo	Enum	ERROR, ALL, INFO, DEBUG	No default value

Este control comprueba si un usuario 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 API solicitudes y las respuestas, 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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un AWS AppSync GraphQL API tiene etiquetas con las claves específicas definidas en el parámetro. `requiredTagKeys` El control falla si GraphQL API 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 falla si el GraphQL API 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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABAC para qué sirve AWS?](#) en la Guía IAM del usuario.

 Note

No añada información de identificación personal (PII) ni otra información confidencial o delicada 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 añadir etiquetas a un AWS AppSync GraphQLAPI, consulte [TagResource](#) en la AWS AppSync API Referencia.

[AppSync.5] AWS AppSync APIs GraphQL no debe autenticarse con claves 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 API clave para interactuar con un AWS AppSync GraphQLAPI. El control falla si un AWS AppSync GraphQL API se autentica con una clave. API

Una API clave es un valor codificado en la aplicación que el AWS AppSync servicio genera al crear un punto final de GraphQL no autenticado. Si esta API clave está comprometida, tu punto final es vulnerable a un acceso no deseado. A menos que respalde una aplicación o un sitio web de acceso público, no recomendamos utilizar una API clave de autenticación.

Corrección

Para configurar una opción de autorización para tu AWS AppSync GraphQLAPI, consulta [Autorización y autenticación](#) en la Guía para AWS AppSync desarrolladores.

[AppSync.6] AWS AppSync API Las cachés 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 una AWS AppSync API caché está cifrada en tránsito. El control falla si la API caché 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 Athena

Estos controles de Security Hub evalúan el servicio y los recursos de Amazon Athena.

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](#).

[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 en los controles 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-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)

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. Puede utilizar el cifrado del servidor con claves administradas por Amazon Simple Storage Service (Amazon S3), el cifrado del servidor con claves de AWS Key Management Service (AWS KMS) o el cifrado 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	Lista de etiquetas que cumplen los requisitos de AWS	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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la 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
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	Lista de etiquetas que cumplen los requisitos de AWS	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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la 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 publica métricas de uso en Amazon CloudWatch. El control falla si el grupo de trabajo no publica métricas de uso en CloudWatch.

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 habilitar o deshabilitar las métricas de consulta para un grupo de trabajo de Athena, consulte [Cómo habilitar las métricas de consulta de CloudWatch en Athena](#) en la Guía del usuario de Amazon Athena.

Controles de Security Hub para AWS Backup

Estos controles de Security Hub evalúan el servicio y los recursos de AWS Backup.

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 puntos de recuperación de [Backup.1] AWS Backup deben estar cifrados en reposo

Requisitos relacionados: NIST.800-53.r5 CP-9(8), NIST.800-53.r5 SI-12

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

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 de recuperación de AWS Backup está cifrado en reposo. Se produce un error en el control si el punto de recuperación no está cifrado en reposo.

Un punto de recuperación de AWS Backup hace referencia a una copia o instantánea específica de los datos que se crean 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 recuperación de AWS Backup, consulte [Encryption for backups in AWS Backup](#) en la Guía para desarrolladores de AWS Backup.

[Backup.2] Los puntos de recuperación de AWS Backup deben etiquetarse

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
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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un punto de recuperación de AWS Backup 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.

Las etiquetas se pueden asignar a los recursos de AWS 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 recursos de AWS. 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 para permitir 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a un punto de recuperación de AWS Backup

1. Abra la consola de AWS Backup 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] Los almacenes de AWS Backup deben etiquetarse

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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un almacén de AWS Backup 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.

Las etiquetas se pueden asignar a los recursos de AWS 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 recursos de AWS. 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 para permitir 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a un almacén de AWS Backup

1. Abra la consola de AWS Backup 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 informes de AWS Backup deben etiquetarse

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
<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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un plan de informes de AWS Backup 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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 para permitir operaciones cuando la

etiqueta de la entidad principal coincide 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a un plan de informes de AWS Backup

1. Abra la consola de AWS Backup 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 copias de seguridad de AWS Backup deben etiquetarse

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
<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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un plan de copias de seguridad de AWS Backup 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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 para permitir 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a un plan de copias de seguridad de AWS Backup

1. Abra la consola de AWS Backup 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 estos 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
<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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si una cola de trabajos de AWS Batch 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
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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si una política de programación de AWS Batch 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
<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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un entorno de procesamiento AWS por lotes 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.

Controles de Security Hub para ACM

Estos controles de Security Hub evalúan el servicio y los recursos AWS Certificate Manager (ACM).

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](#).

[ACM.1] Los certificados importados y ACM emitidos 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), v4.0.1/4.2.1 PCI DSS

Categoría: Proteger > 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 ACM certificado	Entero	De 14 a 365	30

Este control comprueba si un certificado AWS Certificate Manager (ACM) se renueva dentro del período de tiempo especificado. Comprueba tanto los certificados importados como los certificados proporcionados por 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 DNS la validación. 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 importe. Debe renovar los certificados importados manualmente.

Corrección

ACM proporciona una renovación gestionada para tus TLS certificados SSL/emitidos por Amazon. Esto significa que ACM renueva tus certificados automáticamente (si utilizas la DNS validación) o te envía avisos por correo electrónico cuando se acerca el vencimiento del certificado. Estos servicios se proporcionan tanto para ACM certificados públicos como privados.

Para dominios validados por correo electrónico

Cuando un certificado está a 45 días de caducar, 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 los dominios validados por DNS

ACM renueva automáticamente los certificados que utilizan la DNS validación. 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 en la que se indica 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 Guía del AWS Certificate Manager usuario.

[ACM.2] RSA los certificados gestionados 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 RSA certificados gestionados AWS Certificate Manager utilizan una longitud de clave de al menos 2.048 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 2.048 bits para proteger AWS los recursos, ya que la potencia de cálculo se abarata y los servidores se vuelven más avanzados.

Corrección

La longitud mínima de clave para RSA los certificados emitidos por ya ACM es de 2.048 bits. Para obtener instrucciones sobre cómo emitir nuevos RSA certificados con ACM, consulte [Emisión y administración de certificados](#) en la Guía del AWS Certificate Manager usuario.

Si bien ACM 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 a ACM, consulte los [requisitos previos para la importación de certificados](#) en la Guía del AWS Certificate Manager usuario.

[ACM.3] ACM los certificados 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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un certificado 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.

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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni otra información confidencial o delicada 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 añadir etiquetas a un ACM certificado, consulte [Etiquetado de AWS Certificate Manager certificados](#) en la Guía del AWS Certificate Manager usuario.

Controles de Security Hub para AWS CloudFormation

Estos controles de Security Hub evalúan el servicio y los recursos de AWS CloudFormation.

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](#).

[CloudFormation.1] Las pilas de CloudFormation deben integrarse con Simple Notification Service (SNS) (Simple Notification Service)

Important

Security Hub retiró este control en abril de 2024. Para obtener más información, consulte [Registro de cambios en los controles 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 pila de CloudFormation si no hay ninguna notificación de SNS asociada a ella.

La configuración de una notificación de SNS con su pila de CloudFormation ayuda a notificar inmediatamente a las partes interesadas cualquier evento o cambio que se produzca en la pila.

Corrección

Para integrar una pila de CloudFormation y un tema de SNS, consulte [Actualización de pilas directamente](#) en la Guía del usuario de AWS CloudFormation.

[CloudFormation.2] Las pilas de CloudFormation deben etiquetarse

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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si una pila de AWS CloudFormation 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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una pila de CloudFormation, consulte [CreateStack](#) en la Referencia de la API de AWS CloudFormation.

Controles de Security Hub para CloudFront

Estos controles de Security Hub evalúan el CloudFront 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](#).

[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), v4.0.1/2.2.6 PCI DSS

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 un objeto raíz predeterminado configurado.

A veces, un usuario puede solicitar la raíz de la distribución URL 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 deberían 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-1 (NIST.800-53.r5 SC-23), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-7 (1), (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), v4.0.1/4.2.1 PCI DSS

Categoría: Proteger > 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 la 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) 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 función para comprender el perfil de rendimiento y el impacto de la misma TLS.

Corrección

Para cifrar una CloudFront distribución en tránsito, consulte [Requerir la comunicación entre espectadores y CloudFront en la Guía HTTPS para CloudFront](#) desarrolladores de Amazon.

[CloudFront.4] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin

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 HTTP respuesta 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.

[CloudFront.5] CloudFront las distribuciones deberían tener el registro 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 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 NIST.800-53.r5 SC-7 (8), .800-53.r5 SI-4 (20), .800-53.r5 SI-7 (8), NIST v4.0.1/10.4.2 NIST PCI DSS

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 las distribuciones. CloudFront 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 deberían estar habilitadas WAF

Requisitos relacionados: NIST.800-53.r5 AC-4 (21), v4.0.1/6.4.2 PCI DSS

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 versión clásica o a la web. AWS WAF AWS WAF ACLs El control falla si la distribución no está asociada a una webACL.

AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones web y contra APIs los ataques. Le permite configurar un conjunto de reglas, denominado lista de control de acceso

a la web (webACL), que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Asegúrese de que su CloudFront distribución esté asociada a una AWS WAF web ACL para protegerla de ataques malintencionados.

Corrección

Para asociar una AWS WAF web ACL a una CloudFront distribución, consulta [Cómo controlar AWS WAF el acceso a tu contenido](#) en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.7] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 (3), 3, NIST.800-53.r5 SC-1 3, 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 (2) 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::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.

SSLPersonalice o TLS permita a los usuarios acceder al contenido mediante nombres de dominio alternativos. Puede almacenar los certificados personalizados en AWS Certificate Manager (recomendado) o enIAM.

Corrección

Para añadir un nombre de dominio alternativo a una CloudFront distribución mediante un TLS certificadoSSL/personalizado, consulta [Cómo añadir un nombre de dominio alternativo](#) en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.8] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), .800-53.r5 NIST 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 que sea una dirección IP dedicada.

La indicación del nombre de servidor (SNI) es una extensión del TLS protocolo compatible con los navegadores y clientes lanzados después de 2010. Si lo configura CloudFront para atender HTTPS las solicitudes mediante SNI, CloudFront asocia su nombre de dominio alternativo a una dirección IP para cada ubicación perimetral. Cuando un espectador envía una HTTPS solicitud para tu contenido, DNS dirige la solicitud a la dirección IP de la ubicación de borde correcta. La dirección IP de tu nombre de dominio se determina durante la negociación del TLS protocolo de enlace SSL; la dirección IP no está dedicada a tu distribución.

Corrección

Para configurar una CloudFront distribución que se utilice SNI para atender HTTPS solicitudes, consulte [Utilización SNI para atender HTTPS solicitudes \(funciona para la mayoría de los clientes\)](#) en la Guía para CloudFront desarrolladores. Para obtener información sobre SSL los certificados personalizados, consulte [Requisitos para usar TLS certificados SSL/con CloudFront](#).

[CloudFront.9] CloudFront las distribuciones deberían 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),

(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), v4.0.1/4.2.1 NIST.800-53.r5 SC-2 PCI DSS

Categoría: Proteger > 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 están cifrando el tráfico hacia orígenes personalizados. Este control falla en el caso de 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”.

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 que exija el cifrado de una CloudFront conexión, consulta la [sección Requerir la comunicación entre CloudFront y tu origen personalizado en la Guía HTTPS para CloudFront](#) desarrolladores de Amazon.

[CloudFront.10] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes y los 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, (4), NIST.800-53.r5 SC-1 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), v4.0.1/4.2.1 PCI DSS

Categoría: Proteger > 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 SSL protocolos obsoletos para la HTTPS comunicación entre las ubicaciones de CloudFront borde y tus orígenes personalizados. Este control falla si una CloudFront distribución tiene un «CustomOriginConfigwhere OriginSslProtocols includes». SSLv3

En 2015, el Grupo de Trabajo de Ingeniería de Internet (IETF) anunció oficialmente que la SSL versión 3.0 debería quedar obsoleta debido a que el protocolo no era lo suficientemente seguro. Se recomienda utilizar TLSv1 .2 o una versión posterior para la HTTPS comunicación con sus orígenes personalizados.

Corrección

Para actualizar los SSL protocolos de origen de una CloudFront distribución, consulta [Requerir la comunicación entre CloudFront y tu origen personalizado en la Guía HTTPS 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, .800-53.r5 CM-2 (2), v4.0.1/2.2.6 NIST PCI DSS

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 de una CloudFront distribución falla 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 tu cuenta está configurada para apuntar a un depósito que no existe, un tercero malintencionado puede crear el depósito al que se hace referencia y publicar su propio contenido a través de tu 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 al 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 OAC no está configurado para la CloudFront distribución.

Si utiliza un bucket de S3 como origen para su CloudFront distribución, puede activarlo OAC. Esto permite el acceso al contenido del depósito únicamente a través de la CloudFront distribución especificada y prohíbe el acceso directo desde el depósito u otra distribución. Aunque CloudFront es compatible con Origin Access Identity (OAI), OAC ofrece funciones adicionales y las distribuciones que lo utilizan OAI pueden migrar a OAC ellas. Si bien OAI proporciona una forma segura de acceder a S3 Origins, tiene limitaciones, como la falta de compatibilidad con configuraciones de políticas detalladas y con HTTPS solicitudes HTTP/que utilizan este POST método y Regiones de AWS que requieren la AWS firma de la versión 4 (SiGV4). OAI tampoco admite el cifrado con AWS Key Management Service. OAC se basa en la práctica AWS recomendada de utilizar los directores de IAM servicio para autenticarse con orígenes de S3.

Corrección

OACPara configurar una CloudFront distribución con orígenes de S3, consulte [Restringir el acceso a un origen de Amazon S3](#) en la Guía para CloudFront desarrolladores de Amazon.

[CloudFront.14] CloudFront las distribuciones deben estar etiquetadas

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	Lista de etiquetas que cumplen los requisitos de AWS	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.

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. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 CloudFront distribución, consulta Cómo [etiquetar CloudFront distribuciones de Amazon](#) en la Guía para CloudFront desarrolladores de Amazon.

Controles de Security Hub para CloudTrail

Estos controles de Security Hub evalúan el AWS CloudTrail 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](#).

[CloudTrail.1] CloudTrail debe habilitarse y configurarse con al menos un registro multirregional que incluya eventos de administración de lectura y escritura

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/2.1, CIS AWS Foundations Benchmark v1.4.0/3.1, CIS AWS Foundations Benchmark v3.0.0/3.1, NIST.800-53.r5 AC-2 (4), (26), (9), NIST.800-53.r5 AC-4 (9), (22) NIST.800-53.r5 AC-6 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 hay al menos un registro multirregional que capture los eventos de administración de lectura y escritura. AWS CloudTrail El control falla si CloudTrail está deshabilitado o si no hay al menos un CloudTrail registro que capture los eventos de administración de lectura y escritura.

AWS CloudTrail graba AWS API las llamadas de tu cuenta y te entrega los archivos de registro. La información registrada incluye lo siguiente:

- Identidad de la API persona que llama
- Hora de la llamada API
- Dirección IP de origen de la API persona que llama
- Parámetros de solicitud
- Elementos de respuesta devueltos por el Servicio de AWS

CloudTrail proporciona un historial de las AWS API llamadas de una cuenta, incluidas las API llamadas realizadas desde las herramientas de línea de comandos AWS Management Console AWS SDKs,,. El historial también incluye API las llamadas de un nivel superior Servicios de AWS , como AWS CloudFormation.

El historial de AWS API llamadas generado por CloudTrail permite el análisis de seguridad, el seguimiento de los cambios en los recursos y la auditoría 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.
- Si se trata de un registro multirregional, los eventos de administración de todas las operaciones de lectura y escritura garantizan que las operaciones de administración de CloudTrail registros se realicen en todos los recursos de una Cuenta de AWS sola vez.

De forma predeterminada, las CloudTrail rutas que se crean con ellas AWS Management Console son rutas multirregionales.

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 registrar eventos, eventos de gestión o actividad 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 gestión, para API la actividad, elija Leer y escribir.

[CloudTrail.2] CloudTrail debe tener activado el cifrado en reposo

Requisitos relacionados: PCI DSS v3.2.1/3.4, CIS AWS Foundations Benchmark v1.2.0/2.7, Foundations Benchmark v1.4.0/3.7, CIS AWS Foundations Benchmark v3.0.0/3.5, (1), CIS AWS NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 NIST.800-53.r5

AU-9, NIST.800-53.r5 CA-9 (1), (10), .800-53.r5 SI-7 (6), v4.0.1/10.3.2 NIST.800-53.r5 SC-2
NIST.800-53.r5 SC-7 NIST PCI DSS

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 está configurado para utilizar el cifrado del lado del servidor (SSE). AWS KMS key El control falla si no se ha definido KmsKeyId.

Para aumentar la seguridad de sus archivos de CloudTrail registro confidenciales, debe utilizar el [cifrado del lado del servidor con AWS KMS keys \(SSE-KMS\)](#) en los archivos de CloudTrail registro para cifrarlos en reposo. Tenga en cuenta que, de forma predeterminada, los archivos de registro que envían CloudTrail a sus depósitos se cifran mediante el cifrado del [lado del servidor de Amazon con claves de cifrado administradas por Amazon S3 \(-S3\)](#). SSE

Corrección

Para activar el SSE KMS cifrado de los archivos de CloudTrail registro, consulte [Actualizar un registro para usar una KMS clave en la Guía](#) del usuario.AWS CloudTrail

[CloudTrail.3] Debe estar habilitada al menos una CloudTrail ruta

Requisitos relacionados: 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, v3.2.1/10.2.4, v3.2.1/10.2.5, v3.2.1/10.2.6, v3.2.1/10.2.7, v3.2.1/10.3.1, v3.2.1/10.3.2, PCI DSS v3.2.1/10.3.3, v3.2.1/10.3.4, PCI DSS v3.2.1/10.3.5, PCI DSS PCI DSS PCI DSS PCI DSS PCI DSS PCI DSS PCIDSSv3.2.1/10.3.6, 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 una ruta está habilitada en su. AWS CloudTrail Cuenta de AWS El control falla si tu cuenta no tiene al menos una CloudTrail ruta habilitada.

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 revisar la documentación de cada servicio en [los 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 del archivo de CloudTrail registro debe estar habilitada

Requisitos relacionados: PCI DSS v3.2.1/10.5.2, PCI DSS v3.2.1/10.5.5, Foundations Benchmark v1.2.0/2.2, CIS AWS Foundations Benchmark v1.4.0/3.2, Foundations Benchmark v3.0.0/3.2, CIS AWS NIST .800-53.r5 AU-9, .800-53.r5 SI-4, CIS AWS .800-53.r5 SI-7 (1), .800-53.r5 SI-7 (3), .800-53.r5 SI-7 (7), NIST v4.0.1/10.3.2 NIST NIST NIST PCI DSS

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 CloudTrail registro.

CloudTrail la validación del archivo de registro crea un archivo de resumen firmado digitalmente que contiene un hash de cada registro que se CloudTrail escribe en Amazon S3. Puede utilizar

estos archivos de resumen para determinar si un archivo de registro se modificó, se eliminó o no se modificó 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 los archivos de registro proporciona comprobaciones adicionales de integridad de CloudTrail los registros.

Corrección

Para habilitar la validación de los archivos de CloudTrail registro, consulte [Habilitar la validación de la integridad de los archivos de registro CloudTrail](#) en la Guía del AWS CloudTrail usuario.

[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 AWS Foundations Benchmark v1.4.0/3.4, NIST.800-53.r5 AC-2 (4), (26), (9),, NIST.800-53.r5 AC-4 NIST .800-53.r5 SI-20, NIST.800-53.r5 AC-6 .800-53.r5 SI-3 NIST.800-53.r5 SC-7 (8), .800-53.r5 SI-4 (20), NIST .800-53.r5 SI-4 (5), .800-53.r5 SI-4 (5) NIST -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(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 NIST NIST

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 las CloudTrail rutas están configuradas para enviar registros a CloudWatch registros. El control falla si la propiedad CloudWatchLogsLogGroupArn de la ruta está vacía.

CloudTrail graba AWS API las llamadas que se realizan en una cuenta determinada. La información registrada incluye lo siguiente:

- La identidad de la API persona que llama
- La hora de la llamada API
- La dirección IP de origen de la API persona que llama
- Parámetros de solicitudes
- Los elementos de respuesta devueltos por el Servicio de AWS

CloudTrail utiliza Amazon S3 para el almacenamiento y la entrega de archivos de registro. Puede capturar CloudTrail los registros en un depósito de S3 específico para analizarlos a largo plazo. Para realizar un análisis en tiempo real, puede configurar CloudTrail el envío de CloudWatch registros a Logs.

En el caso de un registro que esté habilitado en todas las regiones de una cuenta, CloudTrail envía los archivos de registro de todas esas regiones a un grupo de CloudWatch registros.

Security Hub recomienda enviar CloudTrail los CloudWatch registros a Logs. 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 usar CloudWatch los registros para configurar esto con su Servicios de AWS. Esta recomendación no impide el uso de una solución diferente.

El envío de CloudTrail CloudWatch registros a Logs facilita el registro de actividades históricas y en tiempo real en función del usuarioAPI, 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] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/2.3, Foundations Benchmark v1.4.0/3.3, CIS AWS v4.0.1/1.4.4 PCI DSS

Categoría: Identificar - Registro

Gravedad: crítica

Tipo de recurso: AWS :: S3 :: Bucket

AWS Config regla: Ninguna (regla personalizada de Security Hub)

Tipo de programa: periódico y activado por cambios

Parámetros: ninguno

CloudTrail registra un registro de todas las API llamadas realizadas en su cuenta. Estos archivos de registro se almacenan en un bucket de S3. CIS recomienda aplicar la política de depósitos de S3, o lista de control de acceso (ACL), al depósito 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 puntos débiles en el uso o la configuración de la cuenta afectada.

Para ejecutar esta comprobación, Security Hub utiliza primero una 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 depósito de CloudTrail S3, consulte [Configuración de los ajustes de bloqueo de acceso público para sus depósitos 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 CloudTrail bucket de S3

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/2.6, Foundations Benchmark v1.4.0/3.6, CIS AWS Foundations Benchmark v3.0.0/3.4, v4.0.1/10.2.1 CIS AWS PCI DSS

Categoría: Identificar - Registro

Gravedad: baja

Tipo de recurso: AWS::S3::Bucket

AWS Config regla: 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.

CISrecomienda 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 una lógica personalizada para buscar el depósito 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 varios Cuentas de AWS depósitos de Amazon S3 a un único bucket de destino, Security Hub evalúa este control únicamente con respecto al depósito de destino de la región en la que se encuentra. Esto optimiza sus resultados. Sin embargo, debes activar todas CloudTrail las cuentas que envían registros al depósito 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] las CloudTrail rutas deben estar etiquetadas

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	Lista de etiquetas que cumplen los requisitos de AWS	No default value

Este control comprueba si un AWS CloudTrail sendero 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.

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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABAC para qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 CloudTrail sendero, consulte [AddTags](#) la AWS CloudTrail API Referencia.

Controles de Security Hub para CloudWatch

Estos controles evalúan el servicio Amazon CloudWatch y sus 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](#).

[CloudWatch.1] Debe existir un filtro de métrica de registro y una alarma para el uso del usuario “raíz”

Requisitos relacionados: PCI DSS v3.2.1/7.2.1, CIS AWS Foundations Benchmark v1.2.0/1.1, CIS AWS Foundations Benchmark v1.2.0/3.3, CIS AWS Foundations Benchmark v1.4.0/1.7, CIS AWS Foundations Benchmark v1.4.0/4.3

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::Logs::MetricFilter, AWS::CloudWatch::Alarm, AWS::CloudTrail::Trail, AWS::SNS::Topic

Regla de AWS Config: 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 rastros de CloudTrail 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 de administración de AWS Organizations o la cuenta de administrador delegado de CloudTrail. 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. Cree 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 ruta de CloudTrail que se aplique a todas las 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 registros de CloudWatch Logs que asocie a la ruta de CloudTrail. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulte [Crear un filtro de métricas para un grupo de registros](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{\$.userIdentity.type="Root" && \$.userIdentity.invokedBy NOT EXISTS && \$.eventType != "AwsServiceEvent"}</code>

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, consulte [Creación de una alarma de CloudWatch basada en un filtro por métricas del grupo de registro](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que <i>your-metric-name</i> sea... que...	Mayor/Igual 1

[CloudWatch.2] Asegurar que haya un filtro de métricas de registro y alarma para las llamadas no autorizadas a la API

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.1

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::Logs::MetricFilter, AWS::CloudWatch::Alarm, AWS::CloudTrail::Trail, AWS::SNS::Topic

Regla de AWS Config: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo los registros de CloudTrail a los registros de CloudWatch y estableciendo los filtros de métricas y alarmas correspondientes.

CIS recomienda que cree un filtro de métricas y alarma para llamadas no autorizadas a la API. 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 rastros de CloudTrail 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 de administración de AWS Organizations o la cuenta de administrador delegado de CloudTrail. 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. Cree 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 ruta de CloudTrail que se aplique a todas las 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 registros de CloudWatch Logs que asocie a la ruta de CloudTrail. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulte [Crear un filtro de métricas para un grupo de registros](#) en la Guía del usuario de Amazon CloudWatch. 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, consulte [Creación de una alarma de CloudWatch basada en un filtro por métricas del grupo de registro](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que <i>your-metric-name</i> sea...	Mayor/Igual
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

Regla de AWS Config: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico


Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo los registros de CloudTrail a los registros de CloudWatch 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 rastros de CloudTrail 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 de administración de AWS Organizations o la cuenta de administrador delegado de CloudTrail. 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. Cree 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 ruta de CloudTrail que se aplique a todas las 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 registros de CloudWatch Logs que asocie a la ruta de CloudTrail. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulte [Crear un filtro de métricas para un grupo de registros](#) en la Guía del usuario de Amazon CloudWatch. 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, consulte [Creación de una alarma de CloudWatch basada en un filtro por métricas del grupo de registro](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que <i>your-metric-name</i> sea...	Mayor/Igual
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 AWS

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::Logs::MetricFilter, AWS::CloudWatch::Alarm, AWS::CloudTrail::Trail, AWS::SNS::Topic

Regla de AWS Config: 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 los registros de CloudTrail a CloudWatch Logs 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 rastros de CloudTrail 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 de administración de AWS Organizations o la cuenta de administrador delegado de CloudTrail. 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. Cree 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 ruta de CloudTrail que se aplique a todas las 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 registros de CloudWatch Logs que asocie a la ruta de CloudTrail. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulte [Crear un filtro de métricas para un grupo de registros](#) en la Guía del usuario de Amazon CloudWatch. 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>Create</pre>

Campo	Valor
	<code>ePolicyVersion) (\$.eventName=DeletePolicyVersion) (\$.eventName=AttachRolePolicy) (\$.eventName=DetachRolePolicy) (\$.eventName=AttachUserPolicy) (\$.eventName=DetachUserPolicy) (\$.eventName=AttachGroupPolicy) (\$.eventName=DetachGroupPolicy))}</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, consulte [Creación de una alarma de CloudWatch basada en un filtro por métricas del grupo de registro](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que <i>your-metric-name</i> sea... que...	Mayor/Igual 1

[CloudWatch.5] Asegúrese de que existan un filtro de métrica de registro y una alarma para los cambios de duración de CloudTrail de AWS Config

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.5, CIS Foundations Benchmark v1.4.0/4.5 AWS

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`,
`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

Regla de AWS Config: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo los registros de CloudTrail a los registros de CloudWatch 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 rastros de CloudTrail 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 de administración de AWS Organizations o la cuenta de administrador delegado de CloudTrail. 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. Cree 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 ruta de CloudTrail que se aplique a todas las 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 registros de CloudWatch Logs que asocie a la ruta de CloudTrail. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulte [Crear un filtro de métricas para un grupo de registros](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	{ (\$.eventName=CreateTrail) (\$.eventName=UpdateTrail) (\$.eventName>DeleteTrail) (\$.eventName=StartLogging) (\$.eventName=StopLogging)}
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, consulte [Creación de una alarma de CloudWatch basada en un filtro por métricas del grupo de registro](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que <i>your-metric-name</i> sea... que...	Mayor/Igual 1

[CloudWatch.6] Asegurar que haya un filtro de métricas de registro y alarma de registro para los errores de autenticación de AWS Management Console

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.6, CIS Foundations Benchmark v1.4.0/4.6 AWS

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::Logs::MetricFilter, AWS::CloudWatch::Alarm, AWS::CloudTrail::Trail, AWS::SNS::Topic

Regla de AWS Config: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo los registros de CloudTrail a los registros de CloudWatch 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 rastros de CloudTrail 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 de administración de AWS Organizations o la cuenta de administrador delegado de CloudTrail. 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. Cree 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 ruta de CloudTrail que se aplique a todas las 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 registros de CloudWatch Logs que asocie a la ruta de CloudTrail. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulte [Crear un filtro de métricas para un grupo de registros](#) en la Guía del usuario de Amazon CloudWatch. 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, consulte [Creación de una alarma de CloudWatch basada en un filtro por métricas del grupo de registro](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que <i>your-metric-name</i> sea...	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 AWS

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

Regla de AWS Config: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo los registros de CloudTrail a los registros de CloudWatch 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 rastros de CloudTrail 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 de administración de AWS Organizations o la cuenta de administrador delegado de CloudTrail. 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. Cree 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 ruta de CloudTrail que se aplique a todas las 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 registros de CloudWatch Logs que asocie a la ruta de CloudTrail. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulte [Crear un filtro de métricas para un grupo de registros](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{{\$.eventSource=kms.amazonaws.com}} && {{\$.eventName=Disa</code>

Campo	Valor
	<code>bleKey) (\$.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, consulte [Creación de una alarma de CloudWatch basada en un filtro por métricas del grupo de registro](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que <i>your-metric-name</i> sea... que...	Mayor/Igual 1

[CloudWatch.8] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de bucket S3

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.8, CIS Foundations Benchmark v1.4.0/4.8 AWS

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

Regla de AWS Config: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo los registros de CloudTrail a los registros de CloudWatch 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 rastros de CloudTrail 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 de administración de AWS Organizations o la cuenta de administrador delegado de CloudTrail. 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. Cree 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 ruta de CloudTrail que se aplique a todas las 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 registros de CloudWatch Logs que asocie a la ruta de CloudTrail. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulte [Crear un filtro de métricas para un grupo de registros](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{ (\$.eventSource=s3.amazonaws.com) && ((\$.eventName=PutBucketAcl) (\$.eventName=PutBucketPolicy) (\$.eventName=PutBucketCors) (\$.eventName=PutBucketLifecycle) (\$.eventName=PutBucketReplication) (\$.eventName=Delet</code>

Campo	Valor
	<code>eBucketPolicy) (\$.eventName=DeleteBucketCors) (\$.eventName=DeleteBucketLifecycle) (\$.eventName=DeleteBucketReplication))}</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, consulte [Creación de una alarma de CloudWatch basada en un filtro por métricas del grupo de registro](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que <i>your-metric-name</i> sea... que...	Mayor/Igual 1

[CloudWatch.9] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de configuración de AWS Config

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.9, CIS Foundations Benchmark v1.4.0/4.9 AWS

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

Regla de AWS Config: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo los registros de CloudTrail a los registros de CloudWatch 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 rastros de CloudTrail 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 de administración de AWS Organizations o la cuenta de administrador delegado de CloudTrail. 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. Cree 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 ruta de CloudTrail que se aplique a todas las 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 registros de CloudWatch Logs que asocie a la ruta de CloudTrail. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulte [Crear un filtro de métricas para un grupo de registros](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{ (\$.eventSource=config.amazonaws.com) && (\$.eventName=StopConfigurationRecorder) (\$.eventName=DeleteDeliveryChannel) (\$.eventN</code>

Campo	Valor
	<code>ame=PutDeliveryChannel) (\$.eventName=PutConfigurati onRecorder))}</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, consulte [Creación de una alarma de CloudWatch basada en un filtro por métricas del grupo de registro](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que <i>your-metric-name</i> sea... que...	Mayor/Igual 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 v1.4.0/4.10 AWS

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

Regla de AWS Config: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo los registros de CloudTrail a los registros de CloudWatch 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 rastros de CloudTrail 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 de administración de AWS Organizations o la cuenta de administrador delegado de CloudTrail. 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. Cree 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 ruta de CloudTrail que se aplique a todas las 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 registros de CloudWatch Logs que asocie a la ruta de CloudTrail. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulte [Crear un filtro de métricas para un grupo de registros](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{ (\$.eventName=AuthorizeSecurityGroupIngress) (\$.eventName=AuthorizeSecurityGroupEgress) (\$.eventName=RevokeSecurityGroupIngress) </code>

Campo	Valor
	<code>(\$.eventName=RevokeSecurityGroupEgress) (\$.eventName=CreateSecurityGroup) (\$.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, consulte [Creación de una alarma de CloudWatch basada en un filtro por métricas del grupo de registro](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que <i>your-metric-name</i> sea... que...	Mayor/Igual 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 v1.4.0/4.11 AWS

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

Regla de AWS Config: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo los registros de CloudTrail a los registros de CloudWatch y estableciendo los filtros de métricas y alarmas correspondientes. Las NACL se utilizan como un filtro de paquetes sin estado para controlar el tráfico de entrada y salida para las subredes en una VPC.

CIS recomienda que cree un filtro de métricas y alarma para los cambios realizados a las NACL. La monitorización de estos cambios ayuda a garantizar que los recursos y servicios de AWS 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 4.11 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 rastros de CloudTrail 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 de administración de AWS Organizations o la cuenta de administrador delegado de CloudTrail. 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. Cree 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 ruta de CloudTrail que se aplique a todas las 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 registros de CloudWatch Logs que asocie a la ruta de CloudTrail. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulte [Crear un filtro de métricas para un grupo de registros](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{ (\$.eventName=CreateNetworkAcl) (\$.eventName=CreateNetworkAclEntry) (\$.eventN</code>

Campo	Valor
	ame>DeleteNetworkAcl) (\$.eventName>DeleteNetworkAclEntry) (\$.eventName=ReplaceNetworkAclEntry) (\$.eventName=ReplaceNetworkAclAssociation)}
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, consulte [Creación de una alarma de CloudWatch basada en un filtro por métricas del grupo de registro](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que <i>your-metric-name</i> sea...	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 v1.4.0/4.12 AWS

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::Logs::MetricFilter, AWS::CloudWatch::Alarm, AWS::CloudTrail::Trail, AWS::SNS::Topic

Regla de AWS Config: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo los registros de CloudTrail a los registros de CloudWatch 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 rastros de CloudTrail 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 de administración de AWS Organizations o la cuenta de administrador delegado de CloudTrail. 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. Cree 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 ruta de CloudTrail que se aplique a todas las 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 registros de CloudWatch Logs que asocie a la ruta de CloudTrail. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulte [Crear un filtro de métricas para un grupo de registros](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<code>{{\$.eventName=CreateCustomerGateway}} (\$.eventName>DeleteCustomerGateway) (\$.eventN</code>

Campo	Valor
	ame=AttachInternetGateway) (\$.eventName=CreateInternetGateway) (\$.eventName=DeleteInternetGateway) (\$.eventName=DetachInternetGateway)}
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, consulte [Creación de una alarma de CloudWatch basada en un filtro por métricas del grupo de registro](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que <i>your-metric-name</i> sea... que...	Mayor/Igual 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 v1.4.0/4.13 AWS

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: AWS::Logs::MetricFilter, AWS::CloudWatch::Alarm, AWS::CloudTrail::Trail, AWS::SNS::Topic

Regla de AWS Config: 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 los registros de CloudTrail a CloudWatch Logs 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 rastros de CloudTrail 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 de administración de AWS Organizations o la cuenta de administrador delegado de CloudTrail. 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 de 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. Cree 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 ruta de CloudTrail que se aplique a todas las 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 registros de CloudWatch Logs que asocie a la ruta de CloudTrail. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulte [Crear un filtro de métricas para un grupo de registros](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<pre>{(\$.eventSource=ec2.amazonaws.com) && ((\$.eventName=CreateRoute) (\$.eventName=CreateRouteTable) (\$.eventName=ReplaceRoute) (\$.eventName=ReplaceRouteTableAssociation) (\$.eventName>DeleteRouteTable) (\$.eventName>DeleteRoute) (\$.eventName=DisassociateRouteTable))}</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, consulte [Creación de una alarma de CloudWatch basada en un filtro por métricas del grupo de registro](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que <i>your-metric-name</i> sea... que...	Mayor/Igual 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 v1.4.0/4.14 AWS

Categoría: Detectar - Servicios de detección

Gravedad: baja

Tipo de recurso: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`,
`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

Regla de AWS Config: Ninguna (regla personalizada de Security Hub)

Tipo de programa: Periódico

Parámetros: ninguno

Puede monitorizar las llamadas a la API en tiempo real dirigiendo los registros de CloudTrail a los registros de CloudWatch y estableciendo los filtros de métricas y alarmas correspondientes. Puede tener más de un VPC en una cuenta, y puede crear una interconexión entre dos VPC, lo que permite dirigir el tráfico de red entre VPC.

CIS recomienda que cree un filtro de métricas y alarma para los cambios realizados a las VPC. 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 rastros de CloudTrail 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 de administración de AWS Organizations o la cuenta de administrador delegado de CloudTrail. 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. Cree 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 ruta de CloudTrail que se aplique a todas las 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 registros de CloudWatch Logs que asocie a la ruta de CloudTrail. En el siguiente paso, debe crear el filtro de métricas para ese grupo de registros.

3. Crear un filtro de métricas. Para obtener instrucciones, consulte [Crear un filtro de métricas para un grupo de registros](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Defina el patrón, el patrón de filtro	<pre>{(\$.eventName=CreateVpc) (\$.eventName>DeleteVpc) (\$.eventName=ModifyVpcAttribute) (\$.eventName=AcceptVpcPeeringConnection) (\$.eventName=CreateVpcPeeringConnection) (\$.eventName>DeleteVpcPeeringConnection) (\$.eventName=RejectVpcPeeringConnection) (\$.eventName=AttachClassicLinkVpc) (\$.eventName=DetachClassicLinkVpc) (\$.eventName=DisableVpcClassicLink) (\$.eventName=EnableVpcClassicLink)}</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, consulte [Creación de una alarma de CloudWatch basada en un filtro por métricas del grupo de registro](#) en la Guía del usuario de Amazon CloudWatch. Use los siguientes valores:

Campo	Valor
Condiciones, tipo de umbral	Estático
Siempre que <i>your-metric-name</i> sea...	Mayor/Igual

Campo	Valor
que...	1

[CloudWatch.15] Las alarmas de CloudWatch deben tener configuradas acciones específicas

Categoría: Detectar - Servicios de detección

Requisitos relacionados: 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(1), NIST.800-53.r5 IR-4(5), NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-4(12), NIST.800-53.r5 SI-4(5)

Gravedad: alta

Tipo de recurso: AWS::CloudWatch::Alarm

Regla de AWS Config: [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 está establecido en true y	Booleano	true o false	false

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
actionRequired	la alarma tiene una acción cuando el estado de la alarma cambia a INSUFFICIENT_DATA .			
okActionRequired	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 OK.	Booleano	true o false	false

Este control comprueba si una alarma de Amazon CloudWatch tienen al menos una acción configurada para el estado ALARM. 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 las alarmas de métricas de CloudWatch. 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 alarma de CloudWatch tiene una acción de alarma configurada, mientras [CloudWatch.17](#) se centra en el estado de activación de una acción de alarma de CloudWatch.

Recomendamos que las acciones de alarma de CloudWatch le avisen automáticamente cuando una métrica supervisada 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 compatibles con las alarmas de CloudWatch, consulte [Acciones de alarma](#) en la Guía del usuario de Amazon CloudWatch.

[CloudWatch.16] Los grupos de registros de CloudWatch 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

Regla de AWS Config: [cw-loggroup-retention-period-check](#)

Tipo de programa: Periódico

Parámetros:

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
minRetentionTime	Periodo mínimo de retención en días para los grupos de registros de CloudWatch	Enum	365, 400, 545, 731,	365

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
			1827, 3653	

Este control comprueba si un grupo de registros de Amazon CloudWatch 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.

registros de CloudWatch le permite centralizar los registros de todos los sistemas, aplicaciones y servicios de Servicios de AWS que utilice, en un único servicio de gran escalabilidad. Puede utilizar registros de CloudWatch 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 otros orígenes. Conservar los registros durante al menos un año puede ayudarle a cumplir con los estándares de retención de registros.

Corrección

Para configurar los parámetros de retención de registros, consulte [Cambio de la retención de datos de registros en Registros de CloudWatch](#) en la Guía de usuario de Amazon CloudWatch.

[CloudWatch.17] Las acciones de alarma de CloudWatch deben estar activadas

Categoría: Detectar - Servicios de detección

Requisitos relacionados: 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-2, NIST.800-53.r5 SI-4(12)

Gravedad: alta


Tipo de recurso: AWS::CloudWatch::Alarm

Regla de AWS Config: [cloudwatch-alarm-action-enabled-check](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si están activadas las acciones de alarma de CloudWatch (`ActionEnabled` debe configurarse en `true`). El control falla si la acción de alarma de una alarma de CloudWatch está desactivada.

 Note

Security Hub evalúa este control en función de las alarmas de métricas de CloudWatch. 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 alarma de CloudWatch, mientras que [CloudWatch.15](#) se centra en si hay alguna acción ALARM configurada en una alarma de CloudWatch.

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 alarma de CloudWatch para ayudarle a responder rápidamente a los problemas operativos y de seguridad.

Corrección

Cómo activar una acción de alarma de CloudWatch (consola)

1. Abra la consola de CloudWatch 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 alarma de CloudWatch, consulte [Acciones de alarma](#) en la Guía del usuario de Amazon CloudWatch.

Controles de Security Hub para CodeArtifact

Estos controles de Security Hub evalúan el servicio y los recursos de AWS CodeArtifact.

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](#).

[CodeArtifact.1] Los repositorios de CodeArtifact deben etiquetarse

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
<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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un repositorio de AWS CodeArtifact 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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a un repositorio de CodeArtifact, consulte [Etiquetado de un repositorio en CodeArtifact](#) en la Guía del usuario de AWS CodeArtifact.

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: v3.2.1/8.2.1 NIST.800-53.r5 SA-3, PCI DSS v4.0.1/8.3.2 PCI DSS

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 el repositorio URL 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 el repositorio fuente de Bitbucket URL contiene tokens de acceso personales 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 ni transmitirse en texto sin cifrar ni aparecer en el repositorio de origen. URL En lugar de utilizar fichas de acceso personales o credenciales de inicio de sesión, debes acceder a tu proveedor de origen y cambiar tu repositorio de origen URL 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. Reconfigura tu repositorio URL y los ajustes de configuración adicionales, según sea necesario.
8. Elija Update source (Actualizar origen).

Para obtener más información, consulte 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 v3.2.1/8.2.1 NIST.800-53.r5 SA-3, v4.0.1/8.3.2 PCI DSS

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 CodeBuild proyecto, consulte [Cambiar la configuración de un 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, NIST.800-53.r5 SC-2 8, 8 (1), NIST.800-53.r5 SC-2 NIST .800-53.r5 SI-7 (6), v4.0.1/10.3.2 PCI DSS

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), 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 AU-9(7), NIST.800-53.r5 CA-7, .800-53.r5 SI-4, .800-53.r5 SI-4 (20), NIST .800-53.r5 SI-7 (8) NIST NIST

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 CodeBuild comprueba si el entorno de un proyecto tiene al menos una opción de registro, ya sea para S3 o para registros habilitados. CloudWatch 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 en los controles 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 API las solicitudes 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 y al hardware subyacente del APIs 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 CodGuru Profiler

Estos controles de Security Hub evalúan el CodGuru 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](#).

[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
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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un grupo de CodGuru 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 del CodeGuru revisor.

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	Lista de etiquetas que cumplen los requisitos de AWS	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 Amazon CodeGuru Reviewer, consulte [Etiquetar una asociación de repositorios en Amazon CodeGuru Reviewer](#) en la Guía del usuario de Amazon CodeGuru Reviewer.

Controles de Security Hub para Amazon Cognito

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon Cognito.

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](#).

[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. 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 completamente. 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.

Tras crear un grupo de usuarios de 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 Cognito genere su primer evento.

Corrección

Para activar la protección contra amenazas para un grupo de usuarios de 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.

Las comprobaciones 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](#).

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 cumplimiento de las conclusiones sobre el control](#).

Para obtener una lista de los recursos que deben registrarse para cada control, consulte [AWS Config Recursos necesarios para las conclusiones sobre el control de Security Hub](#). Para obtener información general sobre cómo habilitar AWS Config y configurar el registro de recursos, consulte [Activación y configuración AWS Config de Security Hub](#).

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	Lista de etiquetas que cumplen los requisitos de AWS	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.

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 estar cifrados en reposo

Requisitos relacionados: NIST.800-53.r5 AC-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

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 servidor es una característica de los flujos 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 DataSync

Estos controles de Security Hub evalúan el servicio y los recursos de AWS DataSync.

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](#).

[DataSync.1] Las tareas de DataSync deben tener el registro habilitado

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 tarea de AWS DataSync tiene habilitado 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 configurar el registro de las tareas de DataSync, consulte [Configuring logging for your DataSync transfer task](#) en la Guía del usuario de AWS DataSync.

Controles de Security Hub para Detective

Estos controles de Security Hub evalúan el servicio y los recursos de Amazon Detective.

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](#).

[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
requiredTagKeys	Lista de claves de etiquetas que no corresponden al	StringList	Lista de etiquetas que	No default value

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.		cumplen los requisitos de AWS	

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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 para permitir 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la 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) 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 v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, v3.2.1/1.3.2, v3.2.1/1.3.6, PCI DSS v4.0.1/1.4.4 PCI DSS PCI DSS

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 instancia de replicación VPC mediante una conexión VPN AWS Direct Connect, o VPC interconexión. 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 debe asegurarse de que el acceso a la configuración de la AWS DMS instancia esté limitado únicamente a los usuarios autorizados. Para ello, restrinja los IAM permisos de los usuarios para modificar AWS DMS la configuración y los recursos.

Corrección

No puede cambiar la configuración de acceso público de una instancia de DMS replicación 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] DMS los certificados 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
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	Lista de etiquetas que cumplen los requisitos de AWS	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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 añadir etiquetas a un DMS certificado, consulte [Etiquetar los recursos AWS Database Migration Service en](#) la Guía del AWS Database Migration Service usuario.

[DMS.3] las suscripciones a DMS eventos 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
<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	Lista de etiquetas que cumplen los requisitos de AWS	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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABAC para qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añade información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 añadir etiquetas a una suscripción a un DMS evento, consulte [Etiquetar los recursos AWS Database Migration Service en](#) la Guía del AWS Database Migration Service usuario.

[DMS.4] las instancias de DMS replicación deben estar etiquetadas

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	Lista de etiquetas que cumplen los requisitos de AWS	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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABAC Para qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 añadir etiquetas a una instancia de DMS replicación, consulte [Etiquetar los recursos AWS Database Migration Service en](#) la Guía del AWS Database Migration Service usuario.

[DMS.5] los grupos de subredes de DMS replicación 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
<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	Lista de etiquetas que cumplen los requisitos de AWS	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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la

etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 añadir etiquetas a un grupo de subredes de DMS replicación, consulte [Etiquetar los recursos AWS Database Migration Service en](#) la Guía del usuario.AWS Database Migration Service

[DMS.6] las instancias de DMS replicación deben tener habilitada la actualización automática de las versiones secundarias

Requisitos relacionados: NIST .800-53.r5 SI-2, .800-53.r5 SI-2 (2), NIST .800-53.r5 SI-2 (4), .800-53.r5 SI-2 (5), NIST v4.0.1/6.3.3 NIST PCI DSS

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 AWS DMS está habilitada para una instancia de replicación. El control falla si la actualización automática de la versión secundaria no está habilitada para una instancia de DMS replicación.

DMSproporciona una actualización automática de las versiones secundarias a cada motor de replicación compatible para que pueda conservar su instancia de replicación up-to-date. 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 DMS replicación, las actualizaciones secundarias 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 DMS replicación, consulte [Modificación de una instancia de replicación](#) en la Guía del AWS Database Migration Service usuario.

[DMS.7] las tareas de DMS replicación de 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 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 NIST.800-53.r5 SC-7 (8), .800-53.r5 SI-4 (20), NIST .800-53.r5 SI-7 (8), v4.0.1/10.4.2 NIST PCI DSS

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 `LOGGER_SEVERITY_DEFAULT` registro está habilitado con el nivel de gravedad mínimo para las tareas de replicación y. `DMS TARGET_APPLY 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— Las declaraciones de datos y del 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 de destino.

El registro desempeña un papel fundamental en las tareas de DMS replicación, 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 DMS replicación de las bases 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 DMS replicación de la base de datos de origen deben tener el registro 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 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 NIST.800-53.r5 SC-7 (8), .800-53.r5 SI-4 (20), NIST .800-53.r5 SI-7 (8), v4.0.1/10.4.2 NIST PCI DSS

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 `LOGGER_SEVERITY_DEFAULT` registro está habilitado con el nivel de gravedad mínimo para las tareas de replicación y `DMS SOURCE_CAPTURE 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`— La replicación continua o la captura de datos de cambios (CDC) los datos se capturan de la base de datos o el servicio de origen y se transfieren al componente de `SORTER` servicio.
- `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 DMS replicación, 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 DMS replicación de la base de datos de origen, consulte [Visualización y administración de los registros de AWS DMS tareas](#) en la Guía del AWS Database Migration Service usuario.

[DMS.9] Los DMS puntos finales deben utilizar SSL

Requisitos relacionados: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 3, NIST.800-53.r5 SC-2 3 (3), 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), v4.0.1/4.2.1 PCI DSS

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 SSL conexión. El control falla si el punto final no lo usaSSL.

SSLTLAS conexiones/proporcionan un nivel de seguridad al cifrar las conexiones entre las instancias de DMS replicación y la 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 SSL conexión en sus DMS puntos finales, protege la confidencialidad de los datos durante la migración.

Corrección

Para añadir una SSL conexión a un DMS terminal nuevo o existente, consulte [Utilización SSL con AWS Database Migration Service](#) en la Guía del AWS Database Migration Service usuario.

[DMS.10] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización 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, v4.0.1/7.3.1 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-5 PCI DSS

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 IAM autorización. El control falla si el DMS punto final no tiene habilitada la IAM autorización.

AWS Identity and Access Management (IAM) proporciona un control de acceso detallado en todas partes. AWS ConIAM, puede especificar quién puede acceder a qué servicios y recursos y en qué condiciones. Con IAM las políticas, usted administra los permisos de su personal y sus sistemas para garantizar los permisos con los privilegios mínimos. Al habilitar la IAM autorización en AWS DMS los puntos finales de las bases de datos de Neptune, puede conceder privilegios de autorización IAM a los usuarios mediante un rol de servicio especificado en el parámetro. ServiceAccessRoleARN

Corrección

Para habilitar la IAM autorización en DMS los puntos finales de las bases de datos de Neptune, [consulte Uso de Amazon Neptune como destino en la Guía](#) del AWS Database Migration Service usuario.AWS Database Migration Service

[DMS.11] DMS Los puntos finales de MongoDB deberían tener habilitado un mecanismo de autenticación

Requisitos relacionados:, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-6, v4.0.1/7.3.1 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-5 PCI DSS

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 -1 para MongoDB versión 3.x o posterior. SCRAM SHA 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 DMS los puntos finales de MongoDB, consulte [Uso de MongoDB como fuente en la Guía del usuario](#). AWS DMS

[DMS.12] DMS Los puntos finales de Redis deberían estar habilitados OSS TLS

Requisitos relacionados:, 3 NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-1 v4.0.1/4.2.1 PCI DSS

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 de Redis OSS está configurado con una TLS conexión. El control falla si el punto final no TLS está activado.

TLS proporciona end-to-end seguridad cuando los datos se envían entre aplicaciones o bases de datos a través de Internet. Al configurar el SSL cifrado para su DMS terminal, se habilita 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 SSL cifrado, se puede acceder a los datos confidenciales, lo que se traduce en filtraciones de datos, pérdida de datos u otros incidentes de seguridad.

Corrección

Para habilitar una TLS conexión en los DMS puntos finales de Redis, consulte [Uso de Redis como destino AWS Database Migration Service en la Guía del AWS Database Migration Service usuario](#).

Controles de Security Hub para Amazon DocumentDB

Estos controles de Security Hub evalúan el servicio y los recursos de Amazon DocumentDB (compatible con MongoDB).

Es posible que estos 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: .800-53.r5 SI-12, v4.0.1/3.2.1 NIST PCI DSS

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
minimumBackupReten	El periodo mínimo de retención de copias de seguridad en días	Entero	De 7 a 35	7

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
RetentionPeriod				

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), 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 (9), NIST.800-53.r5 SC-7 v4.0.1/1.4.4 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 PCI DSS

Categoría: Proteger - Configuración de red segura

Gravedad: crítica

Tipo de recurso: AWS::RDS::DBClusterSnapshot, AWS::RDS:DBSnapshot


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 todas las 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), 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, .800-53.r5 SI-4 (20), .800-53.r5 SI-7 (8), NIST v4.0.1/10.3.3 NIST PCI DSS

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.

Controles de Security Hub para DynamoDB

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon DynamoDB.

Es posible que estos controles no estén disponibles en todos. 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
minProvisionedReadCapacity	Número mínimo de unidades de capacidad de lectura provisionadas para el escalado automático de DynamoDB	Entero	De 1 a 40000	Sin valor predeterminado
targetReadUtilization	Porcentaje de uso objetivo de capacidad de lectura	Entero	De 20 a 90	Sin valor predeterminado
minProvisionedWriteCapacity	Número mínimo de unidades de capacidad de escritura provisionadas para el escalado automático de DynamoDB	Entero	De 1 a 40000	Sin valor predeterminado
targetWriteUtilization	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 provisionado 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, .800-53.r5 SI-13 (5) NIST

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 point-in-time recovery (PITR) está habilitado 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 estén PITR habilitadas se pueden restaurar en 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 () deben cifrarse en reposo DAX

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), .800-53.r5 NIST.800-53.r5 SC-7 SI-7 (6) NIST.800-53.r5 SC-2 NIST

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 Amazon DynamoDB Accelerator DAX () está cifrado en reposo. El control produce un error si el DAX clúster 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 API permisos 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 DAX clúster con el cifrado en reposo activado, consulte [Habilitar el cifrado en reposo mediante la Guía AWS Management Console](#) 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, .800-53.r5 SI-13 (5) NIST

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 <code>true</code> y el recurso lo utiliza.	Booleano	<code>true</code> o <code>false</code>	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 Backupél,

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
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	Lista de etiquetas que cumplen los requisitos de AWS	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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 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::DynamoDB::Table

AWS Config regla: [dax-tls-endpoint-encryption](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un clúster de Amazon DynamoDB Accelerator DAX () está cifrado en tránsito, con el tipo de cifrado de punto final establecido en. TLS El control produce un error si el DAX clúster no está cifrado en tránsito.

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 debes permitir que las conexiones cifradas accedan TLS a los clústeres. DAX Sin embargo, el cifrado de los datos en tránsito puede afectar el rendimiento. Debe probar la aplicación con el cifrado activado para comprender el perfil de rendimiento y su impacto TLS.

Corrección

No puedes cambiar la configuración de TLS cifrado después de crear un DAX clúster. Para cifrar un DAX clúster existente, crea uno nuevo con el cifrado en tránsito activado, transfiere el tráfico de la aplicación a ese clúster y, a continuación, elimina 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 evalúan el servicio y los recursos de Amazon Elastic Compute Cloud (Amazon EC2).

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](#).

[EC2.1] Las instantáneas de Amazon EBS no deberían poder restaurarse públicamente

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, NIST.800-53.r5 AC-2 1, NIST.800-53.r5 AC-3 (7), (21), NIST.800-53.r5 AC-3, (11), (16) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (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 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.

[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente

Requisitos relacionados: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/2.1, CIS Foundations Benchmark v1.2.0/4.3, CIS Foundations Benchmark v1.4.0/5.3, CIS AWS Foundations Benchmark v3.0.0/5.4,, (21), (11), (16), (21), (21), (21), (21), (21), (21), (21), (21), (21), (21), (21), (21), (21), (21), (16), (21), (21) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (21), (21) NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (21), AWS AWS 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 adjuntos de Amazon EBS 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.

[EC2.4] 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	Número de días que la instancia puede permanecer detenida antes de generar un resultado fallido. EC2	Entero	De 1 a 365	30

Este control comprueba si una EC2 instancia de Amazon ha estado detenida durante más tiempo del permitido. El control falla si una EC2 instancia se detiene durante más tiempo que el período de tiempo 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 período de tiempo significativo, se crea un riesgo de seguridad porque la instancia no se mantiene activamente (se analiza, se parchea, se actualiza). Si se lanza más adelante, la falta de un mantenimiento adecuado podría provocar problemas inesperados en su AWS entorno. Para mantener una EC2 instancia inactiva de forma segura a lo largo del tiempo, 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 flujo de VPC debe estar habilitado en todas VPCs

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/2.9, CIS AWS Foundations Benchmark v1.4.0/3.9, CIS Foundations Benchmark v3.0.0/3.7, PCI AWS DSS v3.2.1/10.3.3, PCI DSS v3.2.1/10.3.4, PCI DSS v3.2.1/10.3.5, PCI DSS v3.2.1/10.3.6, (26), NIST.800-53.r5 SI-7 (8) NIST.800-53.r5 AC-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

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 los registros de flujo de Amazon VPC se encuentran y están activados. VPCs El tipo de tráfico se ha establecido como Reje ct. El control falla si los registros de flujo de VPC no están habilitados VPCs 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. Después de crear un registro de flujo, puede ver y recuperar sus datos en los CloudWatch registros. Para reducir los costos, también puede enviar los registros de flujo a Amazon S3.

Security Hub recomienda habilitar el registro de flujo para los paquetes rechazados para 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, selecciona Your. VPCs En Filtro, elija Rechazar o Todos.

[EC2.7] El cifrado predeterminado de EBS debe estar activado

Requisitos relacionados: CIS AWS Foundations Benchmark v1.4.0/2.2.1, CIS AWS Foundations Benchmark v3.0.0/2.2.1, (1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-1 3, 8, NIST.800-53.r5 SC-2 8 NIST.800-53.r5 CA-9 (1), (10), NIST.800-53.r5 SI-7 (NIST.800-53.r5 SC-26) 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). El control falla 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: CIS AWS Foundations Benchmark 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 v4.0.1/2.2.6 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 si la versión de metadatos de la instancia está configurada con la versión 2 () del servicio de metadatos de la EC2 instancia. 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 cada EC2 instancia. 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. El control falla 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 acceder desde Internet. Si lanzas la instancia con una dirección IP pública, se puede acceder a ella desde Internet. EC2 Una IPv4 dirección privada es una dirección IP a la que no se puede acceder desde Internet. Puede usar IPv4 direcciones privadas para la comunicación entre EC2 instancias de la misma VPC o de la red privada conectada.

IPv6 las direcciones son únicas a nivel mundial y, por lo tanto, se puede acceder a ellas desde Internet. Sin embargo, de forma predeterminada, todas las subredes tienen el atributo de IPv6 direccionamiento establecido en `false`. 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 EC2 instancias con direcciones IP públicas, puede ocultar las conclusiones de este control. Para obtener más información sobre las opciones de arquitectura de front-end, consulte el [blog de AWS arquitectura](#) o la [serie de AWS vídeos 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 lanzas 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 las nuevas EC2 instancias de la subred reciben una dirección IP pública del conjunto de direcciones públicas. IPv4

Puedes desasociar de tu instancia una dirección IP pública asignada automáticamente. 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, 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, (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

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 enlace de servicio para Amazon EC2 para cada VPC. El control falla si una VPC no tiene un punto de enlace de VPC creado para el servicio de 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 Security Hub no realiza comprobaciones entre cuentas, verá VPCs que FAILED los resultados se comparten entre cuentas. Security Hub recomienda que suprima estos resultados establecidos como FAILED.

Para mejorar la 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 funcionan con una tecnología que le permite acceder a las operaciones de la EC2 API de Amazon de forma privada. AWS PrivateLink Restringe todo el tráfico de red entre tu 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 puedes crear y adjuntar una política de punto final a tu punto de enlace 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 se asignan a una VPC están conectadas a instancias o EC2 a interfaces de red elásticas en uso (). ENIs

Si se detecta un error, es posible que no las haya utilizado. EC2 EIPs

Esto le ayudará a mantener un inventario preciso de los activos de su entorno EIPs de datos de titulares de tarjetas (CDE).

Corrección

Para liberar una EIP no utilizada, consulte [Liberar una dirección IP elástica](#) en la Guía del EC2 usuario de Amazon.

[EC2.13] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 22

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/4.1, PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/2.2.2, (21), (11), (16) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) 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 (5), NIST.800-53.r5 SC-7 PCI DSS v4.0.1/1.3.1 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 : [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. Tras seleccionar un grupo de seguridad en la EC2 consola de Amazon, selecciona Acciones y edita reglas de entrada. Elimine la regla que permite el acceso al puerto 22.

[EC2.14] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 3389

Requisitos relacionados: CIS Foundations Benchmark v1.2.0/4.2, PCI DSS v4.0.1/1.3.1 AWS

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 0.0.0.0/0 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.

[EC2.15] EC2 Las subredes de Amazon no deberían 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 las subredes de 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

Para configurar una subred para que no asigne direcciones IP públicas, consulte [Modificar el atributo de IPv4 direccionamiento público 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), 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 listas de control de acceso a la red (red ACLs) no utilizadas 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 Elastic Fabric (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 usa más de un ENI. Si sus EC2 instancias necesitan tener varias ENIs como parte de un clúster de Amazon EKS, puede suprimir esas conclusiones de control.

Si tiene varias ENIs subredes, puede haber 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 separar una interfaz de red de una EC2 instancia, consulta [Separar una interfaz de red de una instancia](#) en la Guía del EC2 usuario de Amazon.

[EC2.18] Los grupos de seguridad solo deberían permitir el tráfico entrante sin restricciones en los puertos autorizados

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 > 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
<code>authorizeTcpPorts</code>	Lista de puertos TCP autorizados	IntegerList (mínimo de 1 artículo y máximo de 32 artículos)	De 1 a 65535	[80, 443]
<code>authorizeUdpPorts</code>	Lista de puertos UDP autorizados	IntegerList (mínimo de 1 artículo y máximo de 32 artículos)	De 1 a 65535	Sin valor predeterminado

Este control comprueba si un grupo de EC2 seguridad de Amazon permite el tráfico entrante sin restricciones desde 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.
- Si no se utiliza ningún parámetro, se produce un error en el control de los grupos de seguridad que tengan una regla de tráfico entrante sin restricciones.

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 el sufijo /0) aumenta la posibilidad de que se produzcan actividades maliciosas, como hackeos, 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.

[EC2.19] Los grupos de seguridad no deberían permitir el acceso sin restricciones a los puertos de alto riesgo

Requisitos relacionados: NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 SC-7 (11) 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 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Categoría: Proteger > Acceso restringido a la red

Gravedad: crítica

Tipo de recurso: AWS::EC2::SecurityGroup

AWS Config regla: [restricted-common-ports](#)(la regla creada es `vpc-sg-restricted-common-ports`)

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 entrante sin restricciones de un grupo de EC2 seguridad de Amazon es accesible desde los puertos especificados que se consideran de alto 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 sin restricciones (0.0.0.0/0) aumenta las posibilidades de que se produzcan actividades maliciosas, como la piratería informática, denial-of-service los ataques y la 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 paneles de control)
- 8080 (proxy)

- 8088 (puerto HTTP antiguo)
- 8888 (puerto HTTP alternativo)
- 9200 o 9300 () OpenSearch

Corrección

Para eliminar reglas de un grupo de seguridad, consulta [Eliminar reglas de un grupo de seguridad](#) en la Guía del EC2 usuario de Amazon.

[EC2.20] Los dos túneles VPN de una conexión 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)

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 por el que los datos pueden pasar desde la red del cliente hacia o desde una conexión VPN. AWS Site-to-Site 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 la 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 VPN, consulte [Modificación de las opciones del túnel Site-to-Site VPN](#) en la Guía del usuario de la AWS Site-to-Site VPN.

[EC2.21] La red no ACLs debe permitir la entrada desde el 0.0.0.0/0 al puerto 22 o al puerto 3389

Requisitos relacionados: CIS AWS Foundations Benchmark v1.4.0/5.1, CIS AWS Foundations Benchmark v3.0.0/5.1, (21), (1), NIST.800-53.r5 AC-4 (21), (5), PCI DSS NIST.800-53.r5 CA-9 v4.0.1/1.3.1 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 NIST.800-53.r5 SC-7

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 no utilizados deberían eliminarse

Important

RETIRADO DE ESTÁNDARES ESPECÍFICOS: Security Hub eliminó este control el 20 de septiembre de 2023 del estándar AWS Foundational Security Best Practices y del NIST SP

800-53 Rev. 5. Este control 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 monitorear sus grupos de seguridad.

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 conectados 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 interface.

Corrección

Para crear, asignar y eliminar grupos de seguridad, consulta la guía del EC2 usuario de [Grupos de seguridad](#) en 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.

[EC2.24] No se deben usar 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 Amazon Machine Images (AMIs) de Linux utilizan uno de los dos tipos de virtualización: paravirtual (PV) o máquina virtual de hardware (HVM). Las principales diferencias entre la PV y

la HVM AMIs son la forma en que arrancan y si pueden aprovechar las extensiones de hardware especiales (CPU, red y almacenamiento) para obtener un mejor rendimiento.

Históricamente, en muchos casos los clientes que utilizan sistemas fotovoltaicos ofrecían un mejor rendimiento que los de HVM, pero debido a las mejoras en la virtualización de la HVM y a la disponibilidad de controladores fotovoltaicos para los sistemas HVM AMIs, esto ya no es cierto. Para obtener más información, consulte los [tipos de virtualización de las 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 deberían 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 respaldo

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 AWS Backup Vault Lock <code>true</code> y el recurso lo utiliza.	Booleano	<code>true</code> o <code>false</code>	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 se activará si el volumen de EBS está guardado en un almacén AWS Backup cerrado con llave.

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 backup, consulte [Asignación de recursos a un plan de backup](#) en la Guía para AWS Backup desarrolladores.

[EC2.33] Los archivos adjuntos a las pasarelas de EC2 tránsito deben estar etiquetados

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
<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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un archivo adjunto de Amazon EC2 Transit Gateway 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.

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 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 rutas de las pasarelas de EC2 tránsito deben estar etiquetadas

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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si una tabla de rutas 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.

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 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.

Las interfaces de EC2 red deben estar etiquetadas [EC2.35]

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	Lista de etiquetas que cumplen los	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.		requisitos de AWS	

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.

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 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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si una pasarela de EC2 clientes 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.

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 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 estar etiquetadas

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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si una dirección IP EC2 elástica de Amazon 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.

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 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	Lista de etiquetas que cumplen los requisitos de AWS	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.

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 EC2 instancia, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.39] Las pasarelas EC2 de Internet deben estar etiquetadas

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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si una pasarela 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.

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 pasarela de EC2 Internet, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.40] Las pasarelas EC2 NAT deben estar etiquetadas

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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si una pasarela 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.

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 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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si una lista de control de acceso a la red de Amazon EC2 (ACL de red) 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.

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 ACL EC2 de red, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

Las tablas de EC2 rutas deben estar etiquetadas [EC2.42]

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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si una tabla de EC2 rutas 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.

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 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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un 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.

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 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	Lista de etiquetas que cumplen los requisitos de AWS	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.

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 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-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
<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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un 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.

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 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	Lista de etiquetas que cumplen los requisitos de AWS	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.

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 VPC, consulte [Etiquetar los EC2 recursos de Amazon](#) en la Guía EC2 del usuario de Amazon.

[EC2.47] Los servicios de punto final de Amazon VPC deben estar etiquetados

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	Lista de etiquetas que cumplen los requisitos de AWS	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.

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 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 estar etiquetados

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	Lista de etiquetas que cumplen los requisitos de AWS	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.

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 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 estar etiquetadas

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	Lista de etiquetas que cumplen los requisitos de AWS	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.

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 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 pasarelas de EC2 VPN deben estar etiquetadas

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	Lista de etiquetas que cumplen los	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.		requisitos de AWS	

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.

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 puerta de enlace EC2 VPN, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.51] Los puntos finales de EC2 Client VPN deben tener habilitado el registro de conexiones de clientes

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), Nlst.800-53.r5 SI-7 (8), 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 final tiene habilitado 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 pasarelas de EC2 tránsito deben estar etiquetadas

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
<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	Lista de etiquetas que cumplen los requisitos de AWS	No default value

Este control comprueba si una pasarela 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.

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 pasarela de EC2 transporte, consulta Cómo [etiquetar tus EC2 recursos de Amazon](#) en la Guía del EC2 usuario de Amazon.

[EC2.53] los grupos de EC2 seguridad no deberían permitir la entrada desde el 0.0.0.0/0 a los puertos de administración remota del servidor

Requisitos relacionados: CIS AWS Foundations Benchmark 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 desde 0.0.0.0/0 a los puertos de administración remota del servidor (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 un filtrado continuo 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 EC2 de grupo de seguridad para prohibir el tráfico de entrada a los puertos especificados, consulta [Actualizar reglas de grupos de seguridad](#) en la Guía del EC2 usuario de Amazon. Tras seleccionar un grupo de seguridad en la EC2 consola de Amazon, selecciona Acciones y edita 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 desde: :/0 a los puertos de administración remota del servidor

Requisitos relacionados: CIS AWS Foundations Benchmark 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 desde: `::/0` a los puertos de administración remota del servidor (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 un filtrado continuo 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 EC2 de grupo de seguridad para prohibir el tráfico de entrada a los puertos especificados, consulta [Actualizar reglas de grupos de seguridad](#) en la Guía del EC2 usuario de Amazon. Tras seleccionar un grupo de seguridad en la EC2 consola de Amazon, selecciona Acciones y edita 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 enlace de VPC. Si se proporciona, el control falla si los	StringList	Personalice con una o más VPC IDs	Sin valor predeterminado

Parámetro	Obligatorio	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
		servicios especificados en el serviceName parámetro no tienen uno de estos puntos finales de VPC.			

Este control comprueba si una nube privada virtual (VPC) que usted administra tiene un punto de enlace de VPC de interfaz para la API de Amazon ECR. El control falla si la VPC no tiene un punto final 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 puntos de enlace de VPC. Si se proporciona, el control falla si los servicios	StringList	Personalice con uno o más VPC IDs	Sin valor predeterminado

Parámetro	Obligatorio	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
		especificados en el serviceName parámetro no tienen uno de estos puntos finales de VPC.			

Este control comprueba si una nube privada virtual (VPC) que usted administra tiene un punto final de VPC de interfaz para Docker Registry. El control falla si la VPC no tiene un punto final 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 de Amazon VPC IDs para puntos de enlace de VPC. Si se proporciona, el control falla si los servicios	StringList	Personalice con uno o más VPC IDs	Sin valor predeterminado

Parámetro	Obligatorio	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
		especificados en el serviceName parámetro no tienen uno de estos puntos finales de VPC.			

Este control comprueba si una nube privada virtual (VPC) que usted administra tiene un punto final de VPC de interfaz para. AWS Systems Manager El control falla si la VPC no tiene un punto final 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
vpcIds	Opcional	Lista separada por comas de Amazon VPC IDs para puntos de enlace de VPC. Si se proporciona, el control falla si los	StringList	Personalice con una o más VPC IDs	Sin valor predeterminado

Parámetro	Obligatorio	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
		servicios especificados en el serviceName parámetro no tienen uno de estos puntos finales de VPC.			

Este control comprueba si una nube privada virtual (VPC) que usted administra tiene un punto final de VPC de interfaz para AWS Systems Manager los 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
serviceNames	Obligatorio	El nombre del servicio que evalúa el control	Cadena	No personalizable	ssm-incidents
vpcIds	Opcional	Lista separada por comas de Amazon VPC IDs para puntos de enlace de	StringList	Personalice con uno o más VPC IDs	Sin valor predeterminado

Parámetro	Obligatorio	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
		VPC. Si se proporciona, el control falla si los servicios especificados en el <code>serviceName</code> parámetro no tienen uno de estos puntos finales de VPC.			

Este control comprueba si una nube privada virtual (VPC) que usted administra tiene un punto final 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 utilizar la versión 2 () del Servicio de Metadatos de Instancia 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 la versión 2 (IMDSv2) de Instance Metadata Service. 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 activado

Requisitos relacionados: CIS AWS Foundations Benchmark 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 AWS Site-to-Site VPN tiene Amazon CloudWatch Logs habilitado para ambos túneles. El control falla si una conexión Site-to-Site VPN no tiene habilitados CloudWatch los registros para ambos túneles.

AWS Site-to-Site Los registros de VPN le proporcionan una mayor visibilidad de sus despliegues de Site-to-Site VPN. Con esta función, tiene acceso a los registros de conexión Site-to-Site VPN que proporcionan detalles sobre el establecimiento del túnel de seguridad IP (IPsec), las negociaciones sobre el intercambio de claves de Internet (IKE) y los mensajes del protocolo de detección de pares muertos (DPD). **Site-to-Site** Los registros de VPN se pueden publicar en CloudWatch Logs. Esta función proporciona a los clientes una forma única y coherente de acceder a los registros detallados de todas sus conexiones Site-to-Site VPN y analizarlos.

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-bidireccional, 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 de la 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-bidireccional o 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.

Configurar los ajustes de BPA de la VPC para su cuenta en la Región de AWS le permite bloquear los recursos VPCs y las 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 solo de 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.

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 todos 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 controles de ELB estado

Requisitos relacionados: PCI DSS v3.2.1/2.2, .800-53.r5 CP-2 (2) NIST.800-53.r5 CA-7, NIST .800-53.r5 SI-2 NIST

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 las comprobaciones de estado de Elastic Load Balancing (ELB). El control falla si el grupo de Auto Scaling no utiliza comprobaciones de ELB estado.

ELB las comprobaciones de estado ayudan a garantizar que un grupo de Auto Scaling pueda determinar el estado de una instancia en función de las pruebas adicionales proporcionadas por el balanceador de cargas. 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 de disponibilidad 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, NIST.800-53.r5 AC-3 (15), (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, v4.0.1/2.2.6 PCI DSS

Categoría: Proteger - Configuración de red segura

Gravedad: alta

Tipo de recurso: AWS::AutoScaling::LaunchConfiguration

Regla de AWS Config : [autoscaling-launchconfig-requires-imdsv2](#)

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 está configurada como `optional`, que es una configuración que permite una IMDSv1 u otra IMDSv2.

IMDS proporciona datos sobre la instancia que puede usar para configurar o administrar la instancia en ejecución.

La versión 2 IMDS añade nuevas protecciones que no estaban disponibles IMDSv1 para proteger aún más tus EC2 instancias.

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 en los controles de Security Hub](#).

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST .800-53.r5 CM-2, .800-53.r5 CM-2 (2) NIST

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 HTTP PUT respuesta del servicio de metadatos a solo la EC2 instancia la IMDS protege del uso no autorizado.

El campo Time To Live (TTL) del paquete IP se reduce en uno en cada salto. Esta reducción se puede utilizar para garantizar que el paquete no viaje al exteriorEC2. IMDSv2protege EC2 las instancias que pueden estar mal configuradas como enrutadores abiertos, firewalls de capa 3, túneles o NAT dispositivosVPNs, lo que impide que los usuarios no autorizados recuperen los metadatos. ConIMDSv2, 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), 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 v4.0.1/1.4.4 PCI DSS

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.

EC2Las 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, .800-53.r5 CM-2 (2) NIST

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	Lista de etiquetas que cumplen los requisitos de AWS	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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los

recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 (AmazonECR).

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 ECR privados deben tener configurado el escaneo de imágenes

Requisitos relacionados: v4.0.1/6.2.3 NIST.800-53.r5 RA-5, PCI DSS v4.0.1/6.2.4 PCI DSS

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 ECR repositorio privado de Amazon tiene configurado el escaneo de imágenes. El control falla si el ECR repositorio privado no está configurado para el escaneo instantáneo o continuo.

El escaneo de imágenes de ECR permite identificar vulnerabilidades de software en las imágenes de contenedor. La configuración del escaneo de imágenes en ECR los repositorios añade un nivel de verificación de la integridad y seguridad de las imágenes que se almacenan.

Corrección

Para configurar el escaneo de imágenes para un ECR repositorio, consulte [Escaneo de imágenes](#) en la Guía del usuario de Amazon Elastic Container Registry.

[ECR.2] Los repositorios ECR privados deben tener configurada la inmutabilidad de las etiquetas

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST .800-53.r5 CM-2, .800-53.r5 CM-8 (1) NIST

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 privado tiene habilitada la inmutabilidad de etiquetas. ECR Este control falla si un ECR repositorio privado tiene deshabilitada la inmutabilidad de etiquetas. Esta regla se aplica si la inmutabilidad de la etiqueta está habilitada y tiene el valor IMMUTABLE.

Amazon ECR Tag Immutability 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] ECR Los repositorios 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, .800-53.r5 CM-2 (2) NIST

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 ECR repositorio de Amazon tiene configurada al menos una política de ciclo de vida. Este control falla si un ECR repositorio no tiene ninguna política de ciclo de vida configurada.

Las políticas ECR de ciclo de vida de Amazon le permiten especificar la administración del ciclo de vida de las imágenes en 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 ECR públicos 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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un repositorio ECR público de Amazon 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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los

propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni otra información confidencial o delicada 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 añadir etiquetas a un repositorio ECR público, consulte [Etiquetar un repositorio ECR público de Amazon](#) en la Guía del usuario de Amazon Elastic Container Registry.

Controles de Security Hub para Amazon ECS

Estos controles de Security Hub evalúan el servicio y los recursos de Amazon Elastic Container Service (AmazonECS).

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[ECS.1] Las definiciones de ECS tareas de Amazon 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 ECS tarea de Amazon activa con el modo de red de host tiene definiciones de `user` contenedor `privileged` o definiciones. 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 ECS tarea de Amazon.

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] ECS los servicios 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), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 SC-7 (11) NIST.800-53.r5 AC-6 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 ECS los servicios de Amazon están configurados para asignar automáticamente direcciones IP públicas. 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 lanzas tus ECS instancias de Amazon con una dirección IP pública, podrás acceder a tus ECS instancias de Amazon desde Internet. ECS Los servicios de Amazon 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 su clúster que utilice el modo `aws-ec2` de red y especifique `FARGATE` para `requiresCompatibilities`. A continuación, para la configuración informática, 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 ECS tareas no deben compartir el espacio de nombres del proceso del host

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), .800-53.r5 NIST CM-2

Categoría: Identificar > Configuración de recursos

Gravedad: alta

Tipo de recurso: `AWS::ECS::TaskDefinition`

AWS Config regla `ecs-task-definition-pid-mode-check`

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si las definiciones de ECS tareas de Amazon 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 ECS tarea de Amazon.

Un espacio de nombres de ID de proceso (PID) proporciona una separación entre los procesos. Evita que los procesos del sistema sean visibles y PIDs permite su reutilización, incluido 1. PID Si el espacio de PID nombres 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 ECS contenedores deberían 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 `privileged` parámetro de la definición de contenedor de Amazon ECS Task Definitions está establecido en `true`. El control falla si este parámetro es igual a `true`. Este control solo evalúa la última revisión activa de una definición de ECS tarea de Amazon.

Le recomendamos que elimine los privilegios elevados de las definiciones de sus ECS tareas. 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] ECS Los contenedores deben limitarse al acceso de solo lectura a los sistemas de archivos raíz

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 - 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 los ECS contenedores de Amazon están limitados al acceso de solo lectura a los sistemas de archivos raíz montados. El control falla si el parámetro `readonlyRootFilesystem` se establece como `false` o si el parámetro no existe en la definición del contenedor dentro de la definición de la tarea. Este control solo evalúa la última revisión activa de una definición de ECS tarea de Amazon.

Al habilitar esta opción, se reducen los vectores de ataque a la seguridad, ya que no se puede manipular ni escribir en el sistema de archivos de la instancia contenedora a menos que tenga permisos explícitos de lectura y escritura en sus carpetas y directorios del sistema de archivos. Este control también se adhiere al principio de privilegio mínimo.

Corrección

Limitar las definiciones de contenedor al acceso de solo lectura a los sistemas de archivos raíz

1. Abre la consola Amazon ECS Classic en <https://console.aws.amazon.com/ecs/>.
2. En el panel de navegación izquierdo, elija Definiciones de tareas.
3. Seleccione una definición de tarea que contenga definiciones de contenedores que deban actualizarse. Para cada uno, lleve a cabo los siguientes pasos:
 - En el menú desplegable, selecciona Crear nueva revisión con JSON.
 - Añada el parámetro `readonlyRootFilesystem` y configúrelo como `true` en la definición del contenedor dentro de la definición de la tarea.
 - Seleccione Crear.

[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, v4.0.1/8.6.2 PCI DSS

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

Parámetros:

- `secretKeys AWS_SECRET_ACCESS_KEY=, ECS_ENGINE_AUTH_DATA (no personalizable) AWS_ACCESS_KEY_ID`

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 ECS tarea de Amazon.

AWS Systems Manager Parameter Store puede ayudarle 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 medianteSSM, consulte [Creación de parámetros de Systems Manager](#) en la Guía del AWS Systems Manager usuario. 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 ECS tareas 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 ECS tarea activa de Amazon 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 te ayuda a mantener la fiabilidad, la disponibilidad y el rendimiento de AmazonECS. La recopilación de datos de las definiciones de tareas proporciona visibilidad, lo que puede ayudarle a depurar los procesos y encontrar la causa raíz de los errores. Si utilizas una solución de registro que no tiene que estar definida en la definición de la ECS tarea (como una solución de registro de

terceros), puedes desactivar este control después de asegurarte de que tus registros se capturan y entregan correctamente.

Corrección

Para definir una configuración de registro para las definiciones de las ECS tareas de Amazon, consulte [Especificar una configuración de registro en la definición de la tarea](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.10] Los servicios de ECS Fargate deberían ejecutarse en la última versión de la plataforma Fargate

Requisitos relacionados: NIST .800-53.r5 SI-2, .800-53.r5 SI-2 (2), NIST .800-53.r5 SI-2 (4), .800-53.r5 SI-2 (5), v4.0.1/6.3.3 NIST NIST PCI DSS

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 de Amazon ECS Fargate ejecutan la versión más reciente 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] ECS los clústeres 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 utilizan Container Insights. ECS Este control falla si Container Insights no está configurado para un clúster.

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de los ECS clústeres de Amazon. 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 memoriaCPU, 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 función de 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] ECS los servicios 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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un ECS servicio de Amazon 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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABAC para qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 añadir etiquetas a un ECS servicio, consulta Cómo [etiquetar tus ECS recursos de Amazon](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.14] los ECS clústeres deben estar etiquetados

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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un ECS clúster de Amazon 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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 añadir etiquetas a un ECS clúster, consulta Cómo [etiquetar tus ECS recursos de Amazon](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.15] Las definiciones de ECS tareas deben estar etiquetadas

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
<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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si una definición de ECS tarea de Amazon 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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la

etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 añadir etiquetas a una definición de ECS tarea, consulta Cómo [etiquetar tus ECS recursos de Amazon](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

[ECS.16] Los conjuntos de ECS tareas 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 un conjunto de ECS tareas de Amazon está configurado para asignar automáticamente direcciones IP públicas. 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 su conjunto de tareas con una dirección IP pública, podrá acceder a los recursos asociados

al conjunto de tareas desde Internet. ECS Los conjuntos de tareas no deberían 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 ECS tareas para que no utilice una dirección IP pública, consulte [Actualización de una definición de ECS tarea de Amazon mediante la consola en la Guía para desarrolladores de Amazon Elastic Container Service](#).

Controles de Security Hub para Amazon EFS

Estos controles de Security Hub evalúan el servicio y los recursos de Amazon Elastic File System (AmazonEFS).

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 .800-53.r5 SI-7 NIST.800-53.r5 SC-7 (6) NIST

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 aumentar la seguridad de tus datos confidenciales en AmazonEFS, debes crear sistemas de archivos cifrados. Amazon EFS admite el cifrado de los sistemas de archivos en reposo. Puedes activar el cifrado de los datos en reposo al crear un sistema de EFS archivos de Amazon. Para obtener más información sobre el EFS cifrado de Amazon, consulte [Cifrado de datos en Amazon EFS](#) en la Guía del usuario de Amazon Elastic File System.

Corrección

Para obtener más información sobre cómo cifrar un nuevo sistema de EFS archivos de Amazon, consulte [Cifrado de datos en reposo en](#) la Guía del usuario de Amazon Elastic File System.

[EFS.2] EFS Los volúmenes de Amazon deberían 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, .800-53.r5 SI-13 (5) NIST

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 Amazon Elastic File System (AmazonEFS) se han añadido a los planes de backup incluidos AWS Backup. El control falla si los sistemas de EFS archivos de Amazon no están incluidos en los planes de respaldo.

La inclusión de sistemas de EFS archivos en los planes de respaldo le ayuda a proteger sus datos contra la eliminación o la pérdida de datos.

Corrección

Para habilitar las copias de seguridad automáticas para un sistema de EFS archivos de Amazon existente, consulta [Cómo empezar 4: Crear copias de seguridad EFS automáticas de Amazon](#) en la Guía para AWS Backup desarrolladores.

[EFS.3] los puntos de EFS acceso deben establecer 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 EFS acceso de Amazon 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 NFS cliente que usa el punto de acceso usa 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 EFS acceso de Amazon, consulte Imponer un [directorio raíz con un punto de acceso](#) en la Guía del usuario de Amazon Elastic File System.

[EFS.4] los puntos de EFS acceso deben imponer la identidad de un 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 EFS acceso de Amazon están configurados para imponer la identidad de un usuario. Este control falla si no se define la identidad de un POSIX usuario al crear el punto de EFS acceso.

Los puntos de EFS acceso de Amazon son puntos de entrada específicos de la aplicación a un sistema de EFS archivos que facilitan la gestión del acceso de las aplicaciones a los conjuntos de datos compartidos. Los puntos de acceso pueden imponer la identidad de un usuario, incluidos los POSIX grupos de usuarios, para todas las solicitudes del sistema de archivos que se realicen 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 EFS acceso de Amazon, 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 EFS acceso deben estar etiquetados

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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un punto de EFS acceso de Amazon 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. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABAC para qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 EFS acceso, consulte [Etiquetado de EFS los recursos de Amazon](#) en la Guía del usuario de Amazon Elastic File System.

[EFS.6] Los destinos de EFS montaje 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 EFS montaje de Amazon 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 lo creó. Recomendamos crear objetivos de EFS montaje 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 EFS montaje 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 EFS archivos deben tener habilitadas las copias de seguridad automáticas

Categoría: Recuperación > Resiliencia > Respaldos habilitados

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 EFS archivos de Amazon tiene habilitadas las copias de seguridad automáticas. Este control falla si el sistema de EFS archivos 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 EFS archivos, consulte [Hacer copias de seguridad de los sistemas de EFS archivos](#) en la Guía del usuario de Amazon Elastic File System

[EFS.8] los sistemas de EFS archivos 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-filesystem-ct-encrypted](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un sistema de EFS archivos de Amazon 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 nuevo sistema de EFS archivos, 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 y los recursos de Amazon Elastic Kubernetes Service (EKSA 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](#).

[EKS.1] Los puntos finales de los EKS clústeres 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), 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::EKS::Cluster

Regla de AWS Config : [eks-endpoint-no-public-access](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un punto de enlace de un EKS clúster de Amazon es de acceso público. El control falla si un EKS clúster tiene un punto final que es de acceso público.

Cuando creas un clúster nuevo, Amazon EKS crea un punto final para el API servidor de Kubernetes gestionado que utilizas para comunicarte con el clúster. De forma predeterminada, este punto final API del servidor está disponible públicamente en Internet. El acceso al API servidor está protegido mediante una combinación de AWS Identity and Access Management (IAM) y el control de acceso basado en roles () nativo de Kubernetes. RBAC 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 al punto de enlace de un EKS clúster existente, consulte [Modificación del acceso al punto de enlace del clúster](#) en la Guía del EKS usuario de Amazon. Puede configurar el acceso al punto de conexión para un EKS clúster nuevo al crearlo. Para obtener instrucciones sobre cómo crear un nuevo EKS clúster de Amazon, consulta [Cómo crear un EKS clúster de Amazon](#) en la Guía del EKS usuario de Amazon.

[EKS.2] EKS los clústeres deberían ejecutarse en una versión compatible de Kubernetes

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST .800-53.r5 CM-2, .800-53.r5 SI-2, .800-53.r5 SI-2 (2), NIST .800-53.r5 SI-2 (4), NIST .800-53.r5 SI-2 (5), v4.0.1/12.3.4 NIST NIST PCI DSS

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: 1.29` (no personalizable)

Este control comprueba si un clúster de Amazon Elastic Kubernetes Service (EKSA Amazon) se ejecuta en una versión de Kubernetes compatible. El control falla si el EKS clúster se ejecuta en una versión no compatible.

Si tu aplicación no requiere una versión específica de Kubernetes, te recomendamos que utilices la última versión disponible de Kubernetes compatible con tus clústeres. EKS Para obtener más información, consulte el calendario de [lanzamientos de Amazon EKS Kubernetes](#) y el [soporte de EKS versiones de Amazon, así como en FAQ la Guía](#) del usuario de Amazon EKS.

Corrección

Para actualizar un EKS clúster, consulta la [versión de Kubernetes de un EKS clúster de Amazon en la Guía](#) del usuario de Amazon EKS.

[EKS.3] los EKS clústeres deben usar secretos de Kubernetes cifrados

Requisitos relacionados: NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-1 2, NIST.800-53.r5 SC-1 3, .800-53.r5 SI-28, NIST v4.0.1/8.3.2 PCI DSS

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 EKS clúster de Amazon 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 por EBS volumen que está habilitado de forma predeterminada para todos los datos (incluidos los secretos) que se almacenan en etcd como parte de un clúster. EKS El uso del cifrado de secretos en su EKS clúster le permite implementar una estrategia de defensa exhaustiva para las aplicaciones de Kubernetes, ya que cifra los secretos de Kubernetes con una clave que usted defina y administre. KMS

Corrección

Para habilitar el cifrado de secretos en un EKS clúster, consulte [Habilitar el cifrado de secretos en un clúster existente](#) en la Guía del EKS usuario de Amazon.

[EKS.6] EKS los clústeres deben estar etiquetados

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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si un EKS clúster de Amazon 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. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 añadir etiquetas a un EKS clúster, consulta Cómo [etiquetar tus EKS recursos de Amazon](#) en la Guía del EKS usuario de Amazon.

[EKS.7] Las configuraciones de los proveedores de EKS identidad deben estar etiquetadas

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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

Este control comprueba si la configuración de un proveedor de EKS identidad de Amazon tiene etiquetas con las 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. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABAC para qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 añadir etiquetas a las configuraciones de un proveedor de EKS identidad, consulta [Cómo etiquetar tus EKS recursos de Amazon](#) en la Guía del EKS usuario de Amazon.

[EKS.8] EKS los clústeres deben tener habilitado el registro de auditoría

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, .800-53.r5 SI-4, .800-53.r5 SI-4 (20), NIST .800-53.r5 SI-7 (8), NIST v4.0.1/10.2.1 NIST PCI DSS

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 EKS clúster de Amazon tiene activado 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 EKS auditoría de Amazon está habilitado a través de Amazon Security Lake para Cuenta de AWS.

EKSEI registro del plano de control proporciona registros de auditoría y diagnóstico directamente desde el plano de EKS control 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 EKS clúster CloudWatch. El registro proporciona visibilidad del acceso y el rendimiento de EKS los clústeres. Al enviar los registros del plano de EKS control de sus EKS clústeres 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 su EKS clúster, consulte [Habilitar y deshabilitar los registros del plano de control](#) en la Guía del EKS usuario de Amazon.

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 todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[ElastiCache.1] Los clústeres ElastiCache (RedisOSS) 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, .800-53.r5 SI-13 (5) NIST

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 (RedisOSS) tiene programadas copias de seguridad automáticas. 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 (RedisOSS) 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 ElastiCache API.

Corrección

Para programar copias de seguridad automáticas en un clúster ElastiCache (RedisOSS), 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, .800-53.r5 SI-2 (2), NIST .800-53.r5 SI-2 (4), .800-53.r5 SI-2 (5) v4.0.1/6.3.3 NIST NIST PCI DSS

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 ElastiCache réplicas 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 falla 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 (RedisOSS) deben cifrarse en reposo para añadir 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-1 (NIST.800-53.r5 SC-23), NIST.800-53.r5 SC-2 (4), NIST.800-53.r5 SC-7 (1), (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), v4.0.1/4.2.1 PCI DSS

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 (RedisOSS) de versiones anteriores deberían tener Redis activado OSS AUTH

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), v4.0.1/8.3.1 NIST.800-53.r5 AC-6 PCI DSS

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 (RedisOSS) tiene Redis activado. OSS AUTH El control falla si la OSS versión de Redis 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, recomendamos usar el control de acceso basado en roles (). RBAC Como no RBAC es compatible con las versiones de Redis anteriores a la 6.0, este control solo evalúa las versiones que no pueden usar la función. RBAC

Corrección

Para usar Redis AUTH en un grupo de replicación ElastiCache (RedisOSS), consulte [Modificación del AUTH token en un clúster ElastiCache \(RedisOSS\) existente](#) 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::ElastiCache::CacheCluster

Regla de AWS Config : [elasticache-subnet-group-check](#)

Tipo de programa: Periódico

Parámetros: ninguno

Este control comprueba si un ElastiCache clúster está configurado con un grupo de subredes personalizado. El control falla si CacheSubnetGroupName un ElastiCache clúster tiene el valor default.

Al lanzar un ElastiCache clúster, se crea un grupo de subredes predeterminado si aún no existe ninguno. El grupo predeterminado usa subredes de la nube privada virtual predeterminada (VPC). 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 ElastiCache clúster, consulte [Creación de un grupo de subredes](#) en la Guía del ElastiCache 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 .800-53.r5 SI-2 NIST

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 Images (AMI) 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, .800-53.r5 SI-2 (2), NIST .800-53.r5 SI-2 (4), .800-53.r5 SI-2 (5), v4.0.1/6.3.3 NIST NIST PCI DSS

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: v4.0.1/10.4.2 PCI DSS

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 evalúan el servicio y los recursos de Elastic Load Balancing.

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[ELB.1] Application Load Balancer debe configurarse para redirigir todas las HTTP solicitudes 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) 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 SC-8 .800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6) NIST.800-53.r5 SC-8 NIST

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 la redirección está configurada en todos los receptores de Application Load Balancers. HTTP HTTPS HTTP El control falla si alguno de los HTTP oyentes de los balanceadores de carga de aplicaciones no tiene configurada la redirección. HTTP 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 tanto los protocolos como los protocolos. HTTP HTTPS Puedes usar un agente de HTTPS escucha para delegar el trabajo de cifrado y descifrado en tu balanceador de cargas. Para aplicar el cifrado en tránsito, debes usar acciones de redireccionamiento con los balanceadores de carga de aplicaciones para redirigir las HTTP solicitudes de los clientes a una solicitud en el puerto 443. HTTPS

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 HTTP las solicitudes a HTTPS, debe agregar una regla de escucha de Application Load Balancer 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 y, a continuación HTTP, introduzca. **80** En Añadir acción, redirigir a, elija y HTTPS, 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 y HTTP, a continuación, introduzca**80**. En Añadir acción, redirigir a, elija y HTTPS, a continuación, introduzca**443**.

[ELB.2] Los balanceadores de carga clásicos con HTTPS listenersSSL/deben usar un certificado proporcionado por AWS Certificate Manager

Requisitos relacionados: NIST.800-53.r5 AC-1 7 (2), NIST.800-53.r5 IA-5 (1) NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-1 2 (3), 3, NIST.800-53.r5 SC-1 3 (5), NIST.800-53.r5 SC-2 (4), 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 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::ElasticLoadBalancing::LoadBalancer

Regla de AWS Config : [elb-acm-certificate-required](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si el Classic Load Balancer utiliza SSL los certificadosHTTPS/ proporcionados por AWS Certificate Manager (ACM). El control falla si el Classic Load Balancer configurado conHTTPS/SSLlistener no utiliza un certificado proporcionado por. ACM

Para crear un certificado, puede utilizar una herramienta compatible con los TLS protocolos SSL y, por ejemplo, Open. ACM SSL Security Hub recomienda que los utilices ACM para crear o importar certificados para tu balanceador de carga.

ACMse integra con los balanceadores de carga clásicos para que puedas implementar el certificado en tu balanceador de carga. También debe renovar estos certificados automáticamente.

Corrección

Para obtener información sobre cómo asociar un TLS certificado ACMSSL/a un Classic Load Balancer, consulte el artículo del AWS Knowledge Center [¿Cómo puedo asociar un TLS certificado ACMSSL/a un Classic, Application o Network Load Balancer?](#)

[ELB.3] Los oyentes de Classic Load Balancer deben configurarse con o con terminación HTTPS TLS

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), v4.0.1/4.2.1 PCI DSS

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 oyentes de Classic Load Balancer están configurados con HTTPS o con un TLS protocolo para las conexiones front-end (del cliente al balanceador de cargas). 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 Classic Load Balancer están configurados con TLS o HTTPS para conexiones front-end.

El control falla si el oyente no está configurado con TLS o HTTPS para conexiones frontales.

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 debes usar un TLS listener HTTPS o para que el balanceador de cargas se encargue de encriptar y desencriptar en tránsito.

Corrección

Para solucionar este problema, actualiza tus oyentes para que usen el protocolo o. TLS HTTPS

Para cambiar todos los oyentes no conformes a/listeners 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 Load Balancer no esté establecido en SSL o, cámbielo HTTPS a o. HTTPS SSL
6. Para todos los oyentes modificados, en la pestaña Certificados, seleccione Cambiar el valor predeterminado.
7. Para los IAMcertificados ACM y, seleccione un certificado.
8. Seleccione Guardar como predeterminado.
9. Tras actualizar todos los oyentes, selecciona Guardar.

[ELB.4] Application Load Balancer 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), v4.0.1/6.2.4 PCI DSS

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 Application Load Balancer está configurado para eliminar HTTP los encabezados no válidos. El control falla si el valor `routing.http.drop_invalid_header_fields.enabled` se establece como `false`.

De forma predeterminada, los balanceadores de carga de aplicaciones no están configurados para eliminar valores de encabezado no válidos. HTTP La eliminación de estos valores de encabezado evita los ataques de HTTP desincronización.

Note

Recomendamos deshabilitar este control si la opción ELB .12 está habilitada en su cuenta. Para obtener más información, consulte [\[ELB.12\] Application Load Balancer 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 Guardar.

[ELB.5] El registro de aplicaciones y balanceadores 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] Los balanceadores de carga de aplicaciones, puertas de enlace y redes 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: 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 balanceadores de carga clásicos deberían tener habilitado el drenaje de conexiones

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), .800-53.r5 CM-2 NIST

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 balanceadores de carga clásicos que utilizan dispositivos de SSL escucha deben usar una política de seguridad predefinida que tenga una larga duración AWS Config

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), v4.0.1/4.2.1 PCI DSS

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 SSL oyentes o el Classic Load HTTPS Balancer utilizan la política predefinida. ELBSecurityPolicy-TLS-1-2-2017-01 El control falla si no se utiliza el Classic Load BalancerHTTPS/SSLlisteners. ELBSecurityPolicy-TLS-1-2-2017-01

Una política de seguridad es una combinación de SSL protocolos, cifrados y la opción de preferencia de orden de los servidores. Las políticas predefinidas controlan los cifrados, los protocolos y los órdenes de preferencia que se utilizan durante SSL las negociaciones entre un cliente y el balanceador de cargas.

El uso 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 [las políticas de SSL seguridad predefinidas para los balanceadores de carga clásicos](#) en la Guía del usuario de los balanceadores 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 balanceadores de carga clásicos deberían tener activado el balanceo de cargas 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 activado para los balanceadores 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] Classic Load Balancer 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 un Classic Load Balancer se ha configurado para abarcar al menos el número especificado de zonas de disponibilidad (AZs). El control falla si el Classic Load Balancer no

abarca al menos el número especificado de AZs. A menos que proporcione un valor de parámetro personalizado para el número mínimo de AZs, Security Hub usa un valor predeterminado de dos AZs.

Se puede configurar un Classic Load Balancer para distribuir las solicitudes entrantes entre las EC2 instancias de Amazon en una única zona de disponibilidad o en varias zonas de disponibilidad. 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] Application Load Balancer 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), .800-53.r5 CM-2, v4.0.1/6.2.4 NIST PCI DSS

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.

HTTP Los problemas de desincronización 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 balanceadores 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. 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 balanceadores 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 (balanceador de carga de aplicaciones, redes o puertas de enlace) ha registrado instancias de al menos el número especificado de zonas de

disponibilidad (). AZs El control falla si un Elastic Load Balancer V2 no tiene instancias registradas en 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.

Elastic Load Balancing distribuye automáticamente el tráfico entrante entre varios destinos, como EC2 instancias, contenedores y direcciones IP, en una o más 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 Classic Load Balancer 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), .800-53.r5 CM-2, v4.0.1/6.2.4 NIST PCI DSS

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.

HTTPLos problemas de desincronización 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 balanceadores 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. 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 balanceadores de carga de aplicaciones deben estar asociados a una web AWS WAF ACL

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 clásica o AWS WAF web (webACL). 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 y APIs los ataques. Con AWS WAFél, puede configurar una webACL, que es un conjunto de reglas

que permiten, bloquean o cuentan las solicitudes web en función de las reglas y condiciones de seguridad web personalizables que usted defina. Te recomendamos asociar tu Application Load Balancer a AWS WAF una ACL web para protegerla de ataques malintencionados.

Corrección

Para asociar un Application Load Balancer a una webACL, consulte [Asociar o desasociar una web a un AWS recurso en la ACL Guía](#) para desarrolladores.AWS WAF

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 [Cómo 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 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. 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, establezca 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. Seleccione Submit (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 nodos de datos azules o verdes porque hay nodos 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. Seleccione Submit (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 [UpdateDomainConfig](#) Operación de API para configurar el [DomainEndpointOptions](#) objeto. 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
<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	Lista de etiquetas que cumplen los requisitos de AWS	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 estos 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`

Regla de AWS Config : [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 IPv4 dirección pública. De forma predeterminada, 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

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 está cifrada en reposo. El control falla si la configuración de seguridad 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 una configuración de seguridad de Amazon EMR en reposo, [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

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 está cifrada en tránsito. El control falla si la configuración de seguridad 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

Para cifrar una configuración de seguridad de Amazon EMR en tránsito, [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
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	Lista de etiquetas que cumplen los requisitos de AWS	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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABAC para qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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, v4.0.1/10.3.1 PCI DSS

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 todos 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
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	Lista de etiquetas que cumplen los requisitos de AWS	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	Lista de etiquetas que cumplen los requisitos de AWS	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	Lista de etiquetas que cumplen los requisitos de AWS	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	Lista de etiquetas que cumplen los requisitos de AWS	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 estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[FSx.1] FSx para sistemas de ZFS archivos abiertos, debe configurarse para copiar etiquetas a copias de seguridad y volúmenes

Requisitos relacionados: NIST.800-53.r5 CA-9 (1), NIST .800-53.r5 CM-2, .800-53.r5 CM-2 (2) NIST

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 el sistema de ZFS archivos Amazon FSx for Open está configurado para copiar etiquetas a copias de seguridad y volúmenes. El control falla si el sistema de ZFS archivos Open 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 configurar un sistema de ZFS archivos de Open FSx para copiar etiquetas a copias de seguridad y volúmenes, consulte [Actualización de un sistema de archivos](#) en la Guía del ZFS usuario de Amazon FSx for Open.

[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, .800-53.r5 CM-8 NIST

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 configurar un sistema de archivos FSx para que Lustre copie etiquetas a las 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.

Controles de Security Hub para Global Accelerator

Estos controles de AWS Security Hub evalúan el servicio y los recursos de AWS Global Accelerator.

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 etiquetarse

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
requiredTagKeys	Lista de claves de etiquetas que no corresponden al	StringList	Lista de etiquetas que	No default value

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	sistema que debe contener el recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.		cumplen los requisitos de AWS	

Este control comprueba si un acelerador de AWS Global Accelerator tiene etiquetas con las claves 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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la 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 estos 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

AWS Config regla: 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 recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

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. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABAC para qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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.

Controles de Security Hub para GuardDuty

Estos AWS Security Hub controles evalúan el GuardDuty 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](#).

[GuardDuty.1] GuardDuty debe estar activado

Requisitos relacionados: PCI DSS v3.2.1/11.4, PCI DSS v4.0.1/11.5.1, NIST.800-53.r5 AC-2 (12), (4), 1 (1), 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, NIST.800-53.r5 SA-1 5 NIST.800-53.r5 CM-8(3), NIST.800-53.r5 RA-3 (2), 5 (8), (19), (21), (25), (NIST.800-53.r5 SA-11), (3), NIST.800-53.r5 SA-1 .800-53.r5 SI-20, NIST.800-53.r5 SA-8 .800-53.r5 SI-3 NIST.800-53.r5 SA-8 (8), NIST.800-53.r5 SA-8 .800-53.r5 SI-3 NIST.800-53.r5 SC-5 (8) NIST.800-53.r5 SC-5, .800-53.r5 SI-3 NIST.800-53.r5 SC-5 (8) -4, NIST .800-53.r5 SI-4 (1), NIST .800-53.r5 SI-4 (13), .800-53.r5 SI-4 (2), NIST .800-53.r5 SI-4 (22), NIST .800-53.r5 SI-4 (25 NIST NIST NIST NIST), NIST .800-53.r5 SI-4 (4), NIST .800-53.r5 SI-4 (5)

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 activado en tu GuardDuty cuenta y región.

Se recomienda encarecidamente que lo habilites GuardDuty en todas las AWS regiones compatibles. Si lo hace, podrá GuardDuty obtener información sobre actividades no autorizadas o inusuales, incluso en las regiones que no utilice activamente. Esto también permite monitorear CloudTrail eventos GuardDuty a nivel mundial Servicios de AWS , por ejemplo 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
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	Lista de etiquetas que cumplen los requisitos de AWS	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.

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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 GuardDuty filtro, consulte [TagResource](#) en Amazon GuardDuty API Reference.

[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	Lista de etiquetas que cumplen los requisitos de AWS	No default value

Este control comprueba si Amazon GuardDuty IPSet tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. El control falla 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 falla si IPSet 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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABAC Para qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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, consulte GuardDuty IPSet [TagResource](#) en Amazon GuardDuty API Reference.

[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
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	Lista de etiquetas que cumplen los requisitos de AWS	No default value

Este control comprueba si un 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.

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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABAC Para qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 GuardDuty detector, consulte [TagResource](#) en Amazon GuardDuty API Reference.

[GuardDuty.5] La supervisión del registro de GuardDuty EKS auditoría 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 del registro de GuardDuty EKS auditoría está habilitada. En el caso de una cuenta independiente, el control falla si la supervisión del registro de GuardDuty EKS auditoría está deshabilitada en la cuenta. En un entorno con varias cuentas, el control falla si la cuenta de GuardDuty administrador delegado y todas las cuentas de los miembros no tienen habilitada la supervisión del registro de EKS auditoría.

En un entorno con varias cuentas, el control genera resultados únicamente en la cuenta del administrador delegado GuardDuty . Solo el administrador delegado puede activar o desactivar la función de supervisión del registro de EKS auditoría para las cuentas de los miembros de la organización. GuardDuty las cuentas de los 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 del registro de GuardDuty EKS auditoría. Para recibir una PASSED conclusión, el administrador delegado debe desvincular estas cuentas suspendidas. GuardDuty

GuardDuty EKSLa supervisión de registros de auditoría le ayuda a detectar actividades potencialmente sospechosas en sus clústeres de Amazon Elastic Kubernetes Service (Amazon). EKS EKS Audit Log Monitoring utiliza los registros de auditoría de Kubernetes para capturar las actividades cronológicas de los usuarios, las aplicaciones que utilizan Kubernetes y el plano API de control.

Corrección

Para habilitar GuardDuty EKS la supervisión de registros de [EKSAuditoría, consulte Supervisión de registros de auditoría](#) en la Guía del GuardDuty usuario de Amazon.

[GuardDuty.6] La protección GuardDuty Lambda debe estar habilitada

Requisitos relacionados: v4.0.1/11.5.1 PCI DSS

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 GuardDuty Lambda está habilitada. En el caso de una cuenta independiente, el control falla si GuardDuty Lambda Protection está deshabilitada en la cuenta. En un entorno de varias cuentas, el control falla si la cuenta de GuardDuty administrador delegado y todas las cuentas de los miembros no tienen habilitada la Protección Lambda.

En un entorno con varias cuentas, el control genera resultados únicamente en la cuenta de administrador delegado. GuardDuty Solo el administrador delegado puede activar o desactivar la función Lambda Protection para las cuentas de los miembros de la organización. GuardDuty las cuentas de los 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 GuardDuty Lambda. Para recibir una confirmación PASSED, el administrador delegado debe desvincular estas cuentas suspendidas.

GuardDuty

GuardDuty Lambda Protection le ayuda a identificar posibles amenazas de seguridad cuando se invoca una AWS Lambda función. Después de activar Lambda Protection, GuardDuty comienza a monitorear los registros de actividad de la red Lambda asociados a las funciones de Lambda en su. Cuenta de AWS Cuando se invoca una función Lambda e GuardDuty identifica tráfico de red sospechoso que indica la presencia de un fragmento de código potencialmente malicioso en la función Lambda, GuardDuty genera una detección.

Corrección

Para activar GuardDuty Lambda Protection, consulte Configuración de [Lambda Protection en la Guía del usuario](#) de Amazon. GuardDuty

[GuardDuty.7] La monitorización del GuardDuty EKS tiempo de ejecución 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 monitorización del GuardDuty EKS tiempo de ejecución con la gestión automática de agentes está habilitada. En el caso de una cuenta independiente, el control falla si la supervisión del GuardDuty EKS tiempo de ejecución con administración automática de agentes está deshabilitada en la cuenta. En un entorno con varias cuentas, el control falla si la cuenta de GuardDuty administrador delegado y todas las cuentas de los miembros no tienen habilitada EKS Runtime Monitoring con la administración automática de agentes.

En un entorno con varias cuentas, el control genera resultados únicamente en la cuenta del administrador delegado GuardDuty . Solo el administrador delegado puede activar o desactivar la función EKS Runtime Monitoring con una gestión automatizada de los agentes para las cuentas de los miembros de la organización. GuardDuty las cuentas de los 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 monitorización del GuardDuty EKS tiempo de ejecución. Para recibir una PASSED confirmación, el administrador delegado debe desvincular estas cuentas suspendidas. GuardDuty

EKSLa protección en Amazon GuardDuty proporciona una cobertura de detección de amenazas para ayudarlo a proteger los EKS clústeres de Amazon dentro de su AWS entorno. EKS Runtime Monitoring utiliza eventos a nivel del sistema operativo para ayudarlo a detectar posibles amenazas en EKS los nodos y contenedores de sus EKS clústeres.

Corrección

Para habilitar el monitoreo del EKS tiempo de ejecución con la administración automatizada de los agentes, consulte [Habilitar el monitoreo del 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 habilitada. 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 falla si la cuenta de GuardDuty administrador delegado y todas las cuentas de los miembros no tienen habilitada la protección contra malware.

En un entorno con varias cuentas, el control genera resultados únicamente en la cuenta de administrador delegado GuardDuty . Solo el administrador delegado puede activar o desactivar la función de protección contra malware para las cuentas de los miembros de la organización. GuardDuty las cuentas de los 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 una PASSED confirmación, el administrador delegado debe desvincular estas cuentas suspendidas. GuardDuty

GuardDuty Malware Protection for le EC2 ayuda a detectar la posible presencia de malware mediante el escaneo de los volúmenes de Amazon Elastic Block Store (AmazonEBS) adjuntos a las instancias y cargas de trabajo de contenedores de Amazon Elastic Compute Cloud (AmazonEC2). Malware Protection ofrece opciones de análisis con las que puede decidir si desea incluir o excluir EC2 instancias y cargas de trabajo de contenedores específicas en el momento de realizar el escaneo. También ofrece la opción de conservar en sus cuentas las instantáneas de los EBS volúmenes adjuntos a las EC2 instancias o a las cargas de trabajo de los contenedores. 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 malwareEC2, consulte [Configuración del análisis GuardDuty de malware iniciado](#) en la Guía del GuardDuty usuario de Amazon.

[GuardDuty.9] La GuardDuty RDS protección 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 está habilitada. GuardDuty RDS En el caso de una cuenta independiente, el control falla si la GuardDuty RDS protección está deshabilitada en la cuenta. En un entorno con varias cuentas, el control falla si la cuenta de GuardDuty administrador delegado y todas las cuentas de los miembros no tienen RDS habilitada la protección.

En un entorno con varias cuentas, el control genera resultados únicamente en la cuenta del administrador delegado GuardDuty . Solo el administrador delegado puede activar o desactivar la función de RDS protección para las cuentas de los miembros de la organización. GuardDuty las cuentas de los 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 GuardDuty RDS la protección. Para recibir una PASSED confirmación, el administrador delegado debe desvincular estas cuentas suspendidas. GuardDuty

RDSProtection in GuardDuty analiza y perfila la actividad de inicio de RDS sesión para detectar posibles amenazas de acceso a sus bases de datos de Amazon Aurora (Aurora My SQL - Compatible Edition y Aurora Postgre SQL -Compatible Edition). Esta función le permite identificar comportamientos de inicio de sesión potencialmente sospechosos. RDS La protección no requiere una infraestructura adicional; está diseñada para no afectar al rendimiento de las instancias de bases de datos. Cuando RDS Protection detecta un intento de inicio de sesión potencialmente sospechoso o anómalo que indica una amenaza para la base de datos, GuardDuty genera un nuevo hallazgo con detalles sobre la base de datos potencialmente comprometida.

Corrección

Para activar GuardDuty RDS la protección, consulta [GuardDuty RDSProtección](#) en la Guía del GuardDuty usuario de Amazon.

[GuardDuty.10] La protección 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 GuardDuty la protección S3 está habilitada. En el caso de una cuenta independiente, el control falla si GuardDuty S3 Protection está deshabilitada en la cuenta. En un entorno con varias cuentas, el control falla si la cuenta de GuardDuty administrador delegado y todas las cuentas de los miembros no tienen habilitada la protección S3.

En un entorno con varias cuentas, el control genera resultados únicamente en la cuenta del administrador delegado GuardDuty . Solo el administrador delegado puede activar o desactivar la función de protección S3 para las cuentas de los miembros de la organización. GuardDuty las cuentas de los 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 GuardDuty S3. Para recibir una PASSED confirmación, el administrador delegado debe desvincular estas cuentas suspendidas. GuardDuty

S3 Protection permite supervisar API las operaciones GuardDuty a nivel de objeto para identificar posibles riesgos de seguridad para los datos contenidos en sus depósitos de Amazon Simple Storage Service (Amazon S3). GuardDuty monitorea las amenazas contra sus recursos de S3 mediante el análisis de los eventos AWS CloudTrail de administración y los 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.

Controles de Security Hub para IAM

Estos AWS Security Hub controles evalúan el servicio y los recursos AWS Identity and Access Management (IAM).

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](#).

[IAM.1] Las políticas de IAM no deben permitir privilegios administrativos completos “*”

Requisitos relacionados: PCI DSS v3.2.1/7.2.1, CIS AWS Foundations Benchmark v1.2.0/1.22, CIS AWS Foundations Benchmark v1.4.0/1.16,, NIST.800-53.r5 AC-2 (1), (15), (7) NIST.800-53.r5 AC-2,, (10) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (2), NIST.800-53.r5 AC-3 (3) NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6 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 AWS las políticas en línea ni las gestionadas.

Las políticas de IAM definen un conjunto de privilegios concedidos a usuarios, grupos o roles. Siguiendo los consejos de seguridad estándar, se AWS recomienda conceder los privilegios mínimos, es decir, conceder únicamente los permisos necesarios 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 estar activado en todas las regiones en las que utilice 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: PCI DSS v3.2.1/7.2.1, CIS AWS Foundations Benchmark v3.0.0/1.15, CIS Foundations Benchmark v1.2.0/1.16,, (AWS 1), (15), (7) NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (3) NIST.800-53.r5 AC-3 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: 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 los recursos. AWS 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 estar activado en todas las regiones en las que utilice 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: CIS AWS Foundations Benchmark v3.0.0/1.14, CIS Foundations Benchmark v1.4.0/1.14, CIS AWS Foundations Benchmark 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 mejor práctica recomendada es crear una o más AWS IAM Identity Center funciones de IAM o utilizar la federación.](#) 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 necesitan claves de acceso para acceder a AWS los recursos mediante programación.

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 entrada del blog [Pautas para protegerse Cuenta de AWS mientras utiliza el acceso programático.](#)

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 programáticas AWS desde las AWS CLI Herramientas para Windows PowerShell o llamadas HTTP directas mediante las operaciones de la API de forma individual. AWS SDKs Servicios de AWS

Si su organización utiliza AWS IAM Identity Center (IAM Identity Center), sus usuarios pueden iniciar sesión en Active Directory, en un directorio integrado del IAM Identity Center o en [otro proveedor de identidad \(IdP\) conectado al IAM Identity Center](#). A continuación, pueden asignarse a una función de IAM que les permita ejecutar AWS CLI comandos o realizar operaciones de AWS API 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 estar activado en todas las regiones en las que utilice 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: CIS AWS Foundations Benchmark v3.0.0/1.4, CIS AWS Foundations Benchmark v1.4.0/1.4, CIS 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, NIST.800-53.r5 AC-2 (1), (15), (7), (10), (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 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 root es el usuario con más privilegios de un. Cuenta de AWS AWS las claves de acceso proporcionan acceso programático 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 root de una entrada Cuenta de AWS AWS GovCloud (US), consulte [Eliminar las claves de acceso del usuario root de mi AWS GovCloud \(US\) cuenta](#) en la Guía del AWS GovCloud (US) usuario.

[IAM.5] MFA debe estar habilitado para todos los usuarios de IAM que tengan una contraseña de consola

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/1.10, CIS AWS Foundations Benchmark v1.4.0/1.10, CIS AWS Foundations Benchmark v1.2.0/1.2, (1), (15), NIST.800-53.r5 AC-2 (1), (2), NIST.800-53.r5 AC-3 (6), (8), PCI NIST.800-53.r5 IA-2 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 que utilizan una contraseña de consola.

La autenticación multifactor (MFA) agrega una capa adicional de protección además del nombre de usuario y la contraseña. Con la MFA habilitada, cuando un usuario inicia sesión en un AWS sitio web, se le solicita 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 estar activado en todas las regiones en las que utilice 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: CIS AWS Foundations Benchmark v3.0.0/1.6, CIS AWS Foundations Benchmark v1.4.0/1.6, CIS Foundations Benchmark v1.2.0/1.14, PCI AWS DSS v3.2.1/8.3.1, (1), (15), (1), NIST.800-53.r5 AC-2 (1), (2), (6), (8), 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 habilitado para usar un dispositivo de autenticación multifactor (MFA) de hardware para iniciar sesión con credenciales de usuario root. El control falla si la MFA no está habilitada o si se permite que algún dispositivo MFA virtual inicie 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 mientras espera la aprobación de compra de hardware o mientras espera a que llegue su hardware. Para obtener más información, consulte [Habilitación de un dispositivo de autenticación multifactor \(MFA\) virtual \(consola\)](#) en la Guía del usuario de IAM.

Tanto la contraseña temporal de un solo uso (TOTP) como los tokens universales de segundo factor (U2F) son viables como opciones de MFA de hardware.

Corrección

Para añadir un dispositivo MFA de hardware para el usuario root, consulte [Habilitar un dispositivo MFA de hardware para el usuario Cuenta de AWS root \(consola\)](#) 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.](#)

[IAM.7] Las políticas de contraseñas para usuarios de IAM deben tener configuraciones seguras

Requisitos relacionados: NIST.800-53.r5 AC-2 (1), (3), NIST.800-53.r5 AC-2 (15), NIST.800-53.r5 AC-3 (1), PCI DSS NIST.800-53.r5 IA-5 v4.0.1/8.3.6, PCI DSS v4.0.1/8.3.7

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 AWS Management Console acceder a él, 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 función 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 Cuenta de AWS para especificar los requisitos de complejidad y los períodos 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: PCI DSS v3.2.1/8.1.4, PCI DSS v4.0.1/8.2.6, CIS AWS Foundations Benchmark v1.2.0/1.3, (1), (3), (15), (7), NIST.800-53.r5 AC-2 NIST.800-53.r5 AC-2 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 - 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 los recursos mediante distintos tipos de credenciales, como contraseñas o claves de acceso. AWS

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 estar activado en todas las regiones en las que utilice 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, CIS AWS Foundations Benchmark v1.4.0/1.5, CIS Foundations Benchmark v1.2.0/1.13, (AWS 1), (15), (1), (AWS 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

El usuario raíz tiene acceso completo a todos los servicios y recursos en Cuenta de AWS. La MFA aporta una capa adicional de protección además de un nombre de usuario y una contraseña. Con la MFA habilitada, cuando un usuario inicia sesión en el AWS Management Console, se le solicita su nombre de usuario y contraseña y un código de autenticación de su dispositivo de MFA AWS .

Si utiliza la MFA virtual para el usuario raíz, CIS recomienda que el dispositivo utilizado no sea un dispositivo personal. Utilice, en cambio, un dispositivo móvil (tableta o teléfono) que usted mismo administre de modo que se mantenga cargado y protegido independientemente de los dispositivos personales individuales. Esto disminuye el riesgo de perder acceso al dispositivo de MFA debido a pérdida o cambio de dispositivo o a que el propietario del dispositivo ya no esté empleado en la empresa.

Corrección

Para habilitar la MFA para el usuario raíz, consulte Activar la [MFA en el usuario Cuenta de AWS raíz en la Guía de referencia de](#) administración de AWS cuentas.

[IAM.10] Las políticas de contraseñas para los usuarios de IAM deben tener una duración estricta AWS Config

Requisitos relacionados: PCI DSS v3.2.1/8.1.4, PCI DSS v3.2.1/8.2.3, PCI DSS v3.2.1/8.2.4, PCI DSS v3.2.1/8.2.5, 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

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`— Número de días antes de que caduque la contraseña. (Valor predeterminado = 90)

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: CIS AWS Foundations Benchmark v1.2.0/1.5, 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: CIS Foundations Benchmark v1.2.0/1.6, PCI DSS v4.0.1/8.3.6 AWS

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: CIS Foundations Benchmark v1.2.0/1.7, PCI DSS v4.0.1/8.3.6 AWS

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: CIS Foundations Benchmark v1.2.0/1.8, PCI DSS v4.0.1/8.3.6 AWS

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: CIS AWS Foundations Benchmark v3.0.0/1.8, CIS Foundations Benchmark v1.4.0/1.8, CIS Foundations Benchmark v1.2.0/1.9 AWS AWS

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: CIS AWS Foundations Benchmark v3.0.0/1.9, CIS Foundations Benchmark v1.4.0/1.9, CIS Foundations Benchmark v1.2.0/1.10, PCI DSS v4.0.1/8.3.7 AWS AWS

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: CIS AWS Foundations Benchmark v1.2.0/1.11, 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] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/1.17, CIS Foundations Benchmark v1.4.0/1.17, CIS AWS Foundations Benchmark v1.2.0/1.20, PCI DSS v4.0.1/12.10.3
AWS

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 el soporte técnico y el servicio de atención al cliente.

Cree un rol de IAM para permitir que los usuarios autorizados administren incidentes con AWS Support. Al implementar los privilegios mínimos para el control de acceso, una función de IAM

requerirá una política de IAM adecuada que permita el acceso al centro de soporte con el fin de gestionar los incidentes. Soporte

 Note

AWS Config debe estar activado en todas las regiones en las que utilice 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 .

Para crear el rol que se utilizará para el Soporte acceso

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 el campo ID de cuenta, introduzca el Cuenta de AWS ID del usuario Cuenta de AWS al que desea conceder acceso a sus 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 los roles deben ser únicos dentro de 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: PCI DSS v3.2.1/8.3.1, PCI DSS v4.0.1/8.4.2, (1), (15), NIST.800-53.r5 AC-2 (1), (2), NIST.800-53.r5 AC-3 (6), NIST.800-53.r5 IA-2 (8) 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: 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 estar activado en todas las regiones en las que utilice 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 en los controles de Security Hub](#).

Requisitos relacionados: CIS AWS Foundations Benchmark 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 hay restricciones en cuanto al uso del usuario root. Cuenta de AWS El control evalúa los siguientes recursos:

- Temas de Amazon Simple Notification Service (Amazon SNS)
- AWS CloudTrail senderos
- Filtros métricos asociados a los CloudTrail senderos
- 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 CloudTrail existe ningún rastro en la cuenta.

- Una CloudTrail ruta está habilitada, pero no configurada con al menos una ruta multirregional que incluya eventos de administración de lectura y escritura.
- Una CloudTrail ruta está habilitada, pero no está asociada a un grupo de CloudWatch registros.
- 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 existe ninguna CloudWatch alarma basada 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. De forma predeterminada, los registros de la organización son registros multirregionales y solo los puede administrar la cuenta AWS Organizations de administración o la cuenta de CloudTrail administrador 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 problema incluyen la configuración de un tema de Amazon SNS, CloudTrail una ruta, un filtro de métricas y una alarma para el filtro de métricas.

Para crear un tema de Amazon SNS

1. [Abra la consola Amazon SNS en https://console.aws.amazon.com/sns/ la versión 3/home](https://console.aws.amazon.com/sns/la%20versión%203/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.

A continuación, configure una opción 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 multirregional que incluya eventos de administración de lectura y escritura”](#).

Anote el nombre del grupo de CloudWatch registros que asocie a la CloudTrail ruta. 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 que está asociado a la CloudTrail ruta que ha creado.
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 Next (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 Next (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 Next (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 Next (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) 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), NIST.800-53.r5 AC-6 (3)

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 de un Servicio de AWS, excepto a 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.

Al asignar permisos a Servicios de AWS, es importante incluir las acciones de IAM permitidas en sus políticas 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 estar activado en todas las regiones en las que utilice 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: CIS AWS Foundations Benchmark v3.0.0/1.12, CIS Foundations Benchmark v1.4.0/1.12 AWS

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 es igual o superior a 45.

Los usuarios pueden acceder a AWS los recursos mediante 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 estar activado en todas las regiones en las que utilice 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: 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	Lista de etiquetas que cumplen los requisitos de AWS	No default value

Este control comprueba si un analizador gestionado por AWS Identity and Access Management Access Analyzer (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.

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 analizador, consulte [TagResource](#) en la referencia de la AWS API de IAM Access Analyzer.

[IAM.24] Los roles de IAM deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IAM::Role

AWS Config regla: 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	Lista de etiquetas que cumplen los requisitos de AWS	No default value

Este control comprueba si un rol AWS Identity and Access Management (de 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.

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 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: `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
<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	Lista de etiquetas que cumplen los requisitos de AWS	No default value

Este control comprueba si un usuario 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.

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 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: CIS AWS Foundations Benchmark 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

Esto controla si no se elimina un certificado de SSL/TLS server certificate that is managed in IAM has expired. The control fails if the expired SSL/TLS servidor activo.

Para habilitar las conexiones HTTPS a tu sitio web o aplicación AWS, necesitas un certificado de servidor SSL/TLS. Puede usar IAM o AWS Certificate Manager (ACM) para almacenar e implementar certificados de servidor. Utilice IAM como administrador de certificados solo cuando deba admitir conexiones HTTPS en un Región de AWS entorno no 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 el despliegue de certificados de servidor en todas las regiones, pero debe obtener su certificado de un proveedor externo para poder utilizarlo con ellos. 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 la política adjunta AWSCloudShellFullAccess

Requisitos relacionados: CIS Foundations Benchmark v3.0.0/1.22 AWS

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, función o grupo) tiene asociada la política gestionada. AWS AWSCloudShellFullAccess El control lanza error si una identidad de IAM tiene la política AWSCloudShellFullAccess adjunta.

AWS CloudShell proporciona una forma cómoda de ejecutar comandos CLI contra Servicios de AWS. La política AWS gestionada AWSCloudShellFullAccess proporciona acceso total a CloudShell, lo que permite cargar y descargar archivos entre el sistema local del usuario y el CloudShell entorno. Dentro del CloudShell entorno, un usuario tiene permisos de sudo y puede acceder a Internet. Como resultado, adjuntar esta política gestionada a una identidad de IAM les permite instalar software de transferencia de archivos y mover datos desde CloudShell 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: CIS AWS Foundations Benchmark 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 un Cuenta de AWS analizador de acceso externo de IAM Access Analyzer está activado. 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 externos de IAM Access Analyzer ayudan a identificar los recursos, como los buckets de Amazon Simple Storage Service (Amazon S3) o las funciones de 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 los recursos que se comparten con entidades externas, un analizador de acceso utiliza un razonamiento basado en la lógica para analizar las políticas basadas en los recursos de su entorno. AWS Al crear un analizador de acceso externo, puede crearlo y habilitarlo para toda la organización o para 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 [Introducción al analizador de acceso de IAM en la Guía del usuario](#) de 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: v4.0.1/11.3.1 PCI DSS

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 (AmazonEC2) 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 SSM agente, 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 ECR escaneo de Amazon Inspector debe estar activado

Requisitos relacionados: v4.0.1/11.3.1 PCI DSS

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 el ECR escaneo de Amazon Inspector está activado. En el caso de una cuenta independiente, el control falla si el ECR 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 ECR 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 ECR 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 ECR digitalización de Amazon Inspector. Para recibir un resultado PASSED, el administrador delegado debe desvincular estas cuentas suspendidas en Amazon Inspector.

Amazon Inspector escanea las imágenes de los contenedores almacenadas en Amazon Elastic Container Registry (Amazon ECR) en busca de vulnerabilidades de software para generar hallazgos de vulnerabilidades en los paquetes. Cuando activas los escaneos de Amazon Inspector para Amazon ECR, estableces Amazon Inspector como tu servicio de escaneo preferido para tu registro privado. Esto reemplaza el escaneo básico, que Amazon proporciona sin cargo, por el escaneo mejorado ECR, que se proporciona y factura 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. Puedes revisar los hallazgos descubiertos mediante el escaneo mejorado a nivel de imagen, para cada capa de la imagen, en la ECR consola de Amazon. 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 activar el ECR escaneo de Amazon Inspector, consulte [Activación de escaneos](#) 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, v4.0.1/6.3.1 PCI DSS

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, v4.0.1/6.3.1 PCI DSS

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 añade 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 controles de AWS Security Hub evalúan el 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.1] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse

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	Lista de etiquetas que cumplen los requisitos de AWS	No default value

Este control comprueba si un perfil de seguridad de AWS IoT Device Defender 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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a un perfil de seguridad de AWS IoT Device Defender, consulte [Etiquetado de recursos de AWS IoT](#) en la Guía para desarrolladores de AWS IoT.

[IoT.2] Las acciones de mitigación de AWS IoT Core deben etiquetarse

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	Lista de etiquetas que cumplen los requisitos de AWS	No default value

Este control comprueba si una acción de mitigación de AWS IoT Core 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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una acción de mitigación de AWS IoT Core, consulte [Etiquetado de recursos de AWS IoT](#) en la Guía para desarrolladores de AWS IoT.

[IoT.3] Las dimensiones de AWS IoT Core deben etiquetarse

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	Lista de etiquetas que cumplen los requisitos de AWS	No default value

Este control comprueba si una dimensión de AWS IoT Core 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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una dimensión de AWS IoT Core, consulte [Etiquetado de recursos de AWS IoT](#) en la Guía para desarrolladores de AWS IoT.

[IoT.4] Los autorizadores de AWS IoT Core deben etiquetarse

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	Lista de etiquetas que cumplen los requisitos de AWS	No default value

Este control comprueba si un autorizador de AWS IoT Core 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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a un autorizador de AWS IoT Core, consulte [Etiquetado de recursos de AWS IoT](#) en la Guía para desarrolladores de AWS IoT.

[IoT.5] Los alias de los roles de AWS IoT Core deben etiquetarse

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: `AWS::IoT::RoleAlias`

Regla de AWS Config: tagged-iot-rolealiases (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	Lista de etiquetas que cumplen los requisitos de AWS	No default value

Este control comprueba si el alias de un rol de AWS IoT Core tiene etiquetas con las claves específicas definidas en el parámetro `requiredTagKeys`. 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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas al alias de un rol de AWS IoT Core, consulte [Etiquetado de recursos de AWS IoT](#) en la Guía para desarrolladores de AWS IoT.

[IoT.6] Las políticas de AWS IoT Core deben etiquetarse

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	Lista de etiquetas que cumplen los requisitos de AWS	No default value

Este control comprueba si una política de AWS IoT Core 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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una política de AWS IoT Core, consulte [Etiquetado de recursos de AWS IoT](#) en la Guía para desarrolladores de AWS IoT.

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](#).

[Io TEvents .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	Lista de etiquetas que cumplen los requisitos de AWS	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	Lista de etiquetas que cumplen los requisitos de AWS	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.

[IoTEvents .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
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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

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 todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[IoT Site Wise.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 de etiqueta distinguen entre mayúsculas y minúsculas.	StringList	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

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 Site Wise.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
<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	Lista de etiquetas que cumplen los requisitos de AWS	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 Site Wise.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
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	Lista de etiquetas que cumplen los requisitos de AWS	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
<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	Lista de etiquetas que cumplen los requisitos de AWS	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
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	Lista de etiquetas que cumplen los requisitos de AWS	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](#).

[IoTTwinMaker.1] Los trabajos de TwinMaker sincronización de AWS IoT deben estar etiquetados

Categoría: Identificar > Inventario > Etiquetado

Gravedad: baja

Tipo de recurso: AWS::IoTTwinMaker::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
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	Lista de etiquetas que cumplen los requisitos de AWS	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
<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	Lista de etiquetas que cumplen los requisitos de AWS	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 falla 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::IoTTwinMaker::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
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	Lista de etiquetas que cumplen los requisitos de AWS	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
<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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

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 todos 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
<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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

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
<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	Lista de etiquetas que cumplen los requisitos de AWS	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.

[!o TWireless .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	Lista de etiquetas que cumplen los requisitos de AWS	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 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	Lista de etiquetas que cumplen los requisitos de AWS	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
<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	Lista de etiquetas que cumplen los requisitos de AWS	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 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	Lista de etiquetas que cumplen los requisitos de AWS	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 todos 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	Lista de etiquetas que cumplen los requisitos de AWS	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 controles de AWS Security Hub evalúan el servicio Amazon Kinesis y sus 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](#).

[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-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)

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

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
<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	Lista de etiquetas que cumplen los requisitos de AWS	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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 para permitir 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a un flujo de datos de Kinesis, consulte [Etiquetar los 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

Categoría: Recuperación > Resiliencia > Respaldos habilitados

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 [Cambiar el periodo de retención de datos](#) 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 estos controles no estén disponibles en todos 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 de 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 un 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 a 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 devuelve un FAILED resultado AWS KMS key si sus configuraciones AWS Config impiden registrar la política clave en el elemento de configuración (CI) de la clave KMS. 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 está utilizando el rol [AWS Config vinculado al servicio](#).

Corrección

Para obtener información sobre cómo actualizar la política clave de un usuario AWS KMS key, consulte [las políticas clave AWS KMS en](#) la Guía para AWS Key Management Service desarrolladores.

Controles de Security Hub para Lambda

Estos AWS Security Hub controles evalúan el AWS Lambda 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](#).

[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) 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 v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, v3.2.1/1.3.4, v3.2.1/7.2.1, v4.0.1/7.2.1 NIST.800-53.r5 SC-7 PCI DSS PCI DSS PCI DSS

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.

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 Lambda o. API 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, .800-53.r5 SI-2, .800-53.r5 SI-2 (2), NIST .800-53.r5 SI-2 (4), NIST .800-53.r5 SI-2 (5), v4.0.1/12.3.4 NIST NIST PCI DSS

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, dotnet6, java21, java17, java11, java8.al2, nodejs22.x, nodejs20.x, nodejs18.x, python3.13, python3.12, python3.11, python3.10, python3.9, python3.8, ruby3.3, ruby3.2 (no personalizable)

Este control AWS Lambda comprueba si la configuración del tiempo de ejecución de la función coincide con los valores esperados establecidos para los tiempos de ejecución admitidos en cada idioma. El control falla si la función de Lambda no utiliza un tiempo de ejecución compatible, tal como se indicó anteriormente 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 lambda deben estar en un 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), (21), (11), (16) NIST.800-53.r5 AC-3, (20) NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), (3) NIST.800-53.r5 AC-6, (4) 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: 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 una función Lambda está desplegada en una nube privada virtual (VPC). El control falla si la función Lambda no está desplegada en un VPC. Security Hub no evalúa la configuración de enrutamiento de VPC subred para determinar la accesibilidad pública. Es posible que vea resultados erróneos en los recursos de Lambda @Edge.

La implementación de recursos 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 VPC las implementaciones para cumplir con los diversos requisitos de las aplicaciones.

Corrección

Para configurar una función existente para conectarse a sus subredes privadas VPC, consulte [Configuración del VPC acceso](#) en la Guía para AWS Lambda desarrolladores. 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 VPC Lambda 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), .800-53.r5 SI-13 (5) NIST

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 conecten a una VPC deben tener una implementación Multi-AZ para garantizar que una sola zona de fallo no cause una interrupción total de las operaciones.

Corrección

Si configura la función para que se conecte a una VPC de sus cuentas, especifique las subredes en varias AZs para garantizar una alta disponibilidad. Para obtener instrucciones, consulte [Configuración del VPC acceso](#) en la Guía para AWS Lambda desarrolladores.

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	Lista de etiquetas que cumplen los requisitos de AWS	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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABAC Para qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 controles de AWS Security Hub 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-7, NIST.800-53.r5 CA-9(1), NIST.800-53.r5 RA-5, NIST.800-53.r5 SA-8(19), 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), NIST.800-53.r5 RA-5, NIST.800-53.r5 SA-8(19), NIST.800-53.r5 SI-4

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 MSK (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](#).

[MSK.1] MSK Los clústeres deben cifrarse en tránsito entre los nodos intermediarios

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), (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 MSK clúster de Amazon 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 se utiliza TLS para mover 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 en lugar de HTTPS (TLS) conexiones de nodos intermediarios.

Corrección

Para actualizar la configuración de cifrado de MSK los clústeres, consulte [Actualización de la configuración de seguridad de un clúster](#) en la Guía para desarrolladores de Amazon Managed Streaming for Apache Kafka.

[MSK.2] MSK los clústeres deben tener configurada una supervisión mejorada

Requisitos relacionados: NIST.800-53.r5 CA-7 NIST .800-53.r5 SI-2

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 MSK clúster de Amazon tiene configurada la monitorización mejorada, especificada mediante un nivel de monitorización 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 `PER_TOPIC_PER_BROKER` monitoreo proporciona información más detallada sobre el rendimiento del MSK clúster y también proporciona métricas relacionadas con la utilización de los recursos, como CPU el uso de 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 de un MSK clúster, complete los siguientes pasos:

1. ¿Abrir la MSK consola Amazon 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 MSK Connect deben estar cifrados 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 de 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 al crear 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, .800-53.r5 AU-3, .800-53.r5 AU-12, NIST .800-53.r5 SI-4, v4.0.1/10.3.3 NIST NIST PCI DSS

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, .800-53.r5 SI-2, v4.0.1/6.3.3 NIST PCI DSS

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 [Actualización automática de la versión secundaria del motor](#) 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
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	Lista de etiquetas que cumplen los requisitos de AWS	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 recurso y consta de una clave y un valor opcional. AWS 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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 los [recursos de etiquetado](#) 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, NIST.800-53.r5 SC-5 (2), .800-53.r5 SI-13 (5 NIST

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 broker de RabbitMQ, cada uno con su propio volumen de Amazon Elastic Block Store (AmazonEBS) 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), NIST.800-53.r5 AC-4 (26), 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, .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), .800-53.r5 SI-7 (8), NIST v4.0.1/10.3.3 NIST PCI DSS

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 las 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 Neptune en Amazon 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),, NIST.800-53.r5 AC-4 (21) 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 v4.0.1/1.4.4 PCI DSS

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 y API](#) en la Guía del usuario de Amazon Aurora. CLI

[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 período de retención de las copias de seguridad para sus clústeres de bases de datos de Neptune, consulte [Habilitar las copias de seguridad automatizadas](#) en la Guía RDS del usuario de Amazon. Para el período 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 bases de datos de Neptune deben tener habilitada la autenticación de bases de datos IAM

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-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 IAM bases de datos. El control falla si la autenticación IAM de la base de datos no está habilitada para un clúster de base de datos de Neptune.

IAM la autenticación de bases de datos para los clústeres de bases de datos de Amazon Neptune elimina la necesidad de almacenar las credenciales de usuario en la configuración de la base de datos, ya que la autenticación se administra externamente mediante IAM. Cuando la autenticación IAM de bases de datos está habilitada, cada solicitud debe firmarse con la versión 4 de AWS Signature.

Corrección

De forma predeterminada, la autenticación IAM de bases de datos está deshabilitada al crear un clúster de base de datos de Neptune. Para habilitarlo, consulte [Habilitar la autenticación de IAM bases de datos 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, .800-53.r5 CM-2 (2) NIST

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 las instantáneas de la misma forma que sus clústeres de RDS bases de datos principales de Amazon. 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: 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 : [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 Network Firewall

Estos controles de AWS Security Hub evalúan el servicio y los recursos de AWS Network Firewall.

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](#).

[NetworkFirewall.1] Los 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-36, 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 (AZ). Se produce un error en el control si un firewall se implementa en una sola AZ.

La infraestructura global de AWS incluye varias Regiones de AWS. Las AZ 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 AZ, puede equilibrar y desviar el tráfico entre las AZ, lo que ayuda a diseñar soluciones de alta disponibilidad.

Corrección

Implementación de un firewall de Network Firewall en varias zonas de disponibilidad

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 AZ.
7. Seleccione Guardar.

[NetworkFirewall.2] El registro de Network Firewall debe estar habilitado

Requisitos relacionados: NIST.800-53.r5 AC-2(12), 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 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 SC-7(9), NIST.800-53.r5 SI-3(8), 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::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 firewall de AWS Network Firewall. 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

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

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), 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(5)

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.

[NetworkFirewall.7] Los firewall 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
<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	Lista de etiquetas que cumplen los requisitos de AWS	No default value

Este control comprueba si un firewall de AWS Network Firewall tiene etiquetas con 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 recursos de AWS 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 lo 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 recursos de AWS. 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a un firewall de Network Firewall, consulte [Etiquetado de recursos de AWS Network Firewall](#) en la Guía para desarrolladores de AWS Network Firewall.

[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	Lista de etiquetas que cumplen los requisitos de AWS	No default value

Este control comprueba si una política de firewall de AWS Network Firewall tiene etiquetas con 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 recursos de AWS 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 lo 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 recursos de AWS. 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una política de Network Firewall, consulte [Etiquetado de recursos de AWS Network Firewall](#) en la Guía para desarrolladores de AWS Network Firewall.

Los firewalls de Network Firewall [NetworkFirewall.9] 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: Protección > 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 firewall de AWS Network Firewall tiene habilitada la protección contra 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 (VPC), 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 API [UpdateFirewallDeleteProtection](#) y configurando el campo `DeleteProtection` como `true`.

Controles de Security Hub para el OpenSearch servicio

Estos AWS Security Hub controles evalúan el OpenSearch servicio y los recursos de Amazon OpenSearch Service (Servicio).

Es posible que estos controles no estén disponibles en todos 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. 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 falla si un OpenSearch dominio no tiene habilitado 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 solicitudes OpenSearch, 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`.

Un OpenSearch dominio requiere al menos tres nodos de datos para una alta disponibilidad y tolerancia a errores. 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. Seleccione Submit (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 final 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 recurso evaluado. Las claves de etiqueta distinguen entre mayúsculas y minúsculas.	StringList	Lista de etiquetas que cumplen los requisitos de AWS	No default value

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
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	Lista de etiquetas que cumplen los requisitos de AWS	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 estos 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: (Alert, Audit, Trace, Listener)
- PostgreSQL: (Postgresql, Upgrade)
- MySQL: (Auditoría, Error, General, SlowQuery)
- MariaDB: (Auditoría, error, general,) SlowQuery
- SQL Server: (Error, Agent)
- Aurora: (Auditoría, error, general, SlowQuery)
- Aurora-MySQL: (Auditoría, error, general,) SlowQuery

- Aurora-PostgreSQL: (Postgresql, Upgrade).

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 publicar los registros de la base 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	Booleano	No personalizable	false

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	de seguridad para las réplicas de lectura			

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.

Al habilitar las actualizaciones automáticas de las versiones secundarias, se garantiza que se instalen las últimas actualizaciones de las versiones secundarias del sistema de administración de bases de datos relacionales (RDBMS). 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 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

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) 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), (4), 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

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: Nlst.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

Campo	Valor
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
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 una bóveda AWS Backup cerrada 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-dbc1uster` (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	Lista de etiquetas que cumplen los requisitos de AWS	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
<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	Lista de etiquetas que cumplen los requisitos de AWS	Sin valor predeterminado

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	Lista de etiquetas que cumplen los requisitos de AWS	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	Lista de etiquetas que cumplen los requisitos de AWS	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	Lista de etiquetas que cumplen los requisitos de AWS	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	Lista de etiquetas que cumplen los requisitos de AWS	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 un análisis de los datos de registro en tiempo real. 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](#).

Controles de Security Hub para Amazon Redshift

Estos AWS Security Hub controles evalúan el servicio y los recursos de Amazon Redshift.

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](#).

[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) 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 PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, v3.2.1/1.3.4, v3.2.1/1.3.6, v4.0.1/1.4.4 NIST.800-53.r5 SC-7 PCI DSS PCI DSS PCI DSS

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. Cuando el clúster se configura con `PubliclyAccessible` set en `true`, se trata de una instancia con acceso a Internet que tiene un DNS nombre que se puede resolver públicamente, que se resuelve en una dirección IP pública.

Cuando el clúster no es de acceso público, se trata de una instancia interna con un DNS nombre 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), (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::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`.

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 TLS deben permitir las conexiones cifradas a través de redes. El cifrado de los datos en tránsito puede afectar al rendimiento. Debe probar su aplicación con esta función para comprender el perfil de rendimiento y el impacto de la misma 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), NIST.800-53.r5 SC-7 (10), NIST .800-53.r5 SI-13 (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
MinRetencionPeriod	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), (26), NIST.800-53.r5 AC-4 (9), NIST .800-53.r5 SI-3 NIST.800-53.r5 AC-6 (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, .800-53.r5 SI-4 NIST.800-53.r5 SC-7 (20), .800-53.r5 SI-7 (8), NIST v4.0.1/10.2.1 NIST PCI DSS

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
```

[Redshift.7] Los clústeres de Redshift deberían utilizar un enrutamiento mejorado VPC

Requisitos relacionados: NIST.800-53.r5 AC-4 NIST.800-53.r5 AC-4 (21), (11) 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 (4), NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 SC-7

Categoría: Proteger > Configuración de red segura > Acceso API privado

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 VPC enrutamiento mejorado obliga a que todo COPY el UNLOAD tráfico entre el clúster y los repositorios de datos pase por ustedVPC. A continuación, puede utilizar VPC funciones como grupos de seguridad y listas de control de acceso a la red para proteger el tráfico de la red. También puede utilizar los registros de VPC flujo para supervisar el tráfico de la red.

Corrección

Para obtener instrucciones de corrección detalladas, consulte [Habilitar el VPC enrutamiento 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), .800-53.r5 NIST 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: NIST.800-53.r5 CA-9 (1), .800-53.r5 CM-2 NIST

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 condiciones de política. 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, NIST.800-53.r5 SC-2 8, 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::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 KMS cifrado, 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	Lista de etiquetas que cumplen los requisitos de AWS	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. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABAC para qué sirve AWS?](#) en la Guía IAM del usuario.

 Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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-eventssubscription (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	Lista de etiquetas que cumplen los requisitos de AWS	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. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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
<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	Lista de etiquetas que cumplen los requisitos de AWS	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. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la

etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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-clustersubnetgroup (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	Lista de etiquetas que cumplen los	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.		requisitos de AWS	

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. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABAC para qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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: v4.0.1/1.3.1 PCI DSS

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 de grupos de seguridad](#) en la Guía del usuario de VPCAmazon. 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.

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
<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	Lista de etiquetas que cumplen los requisitos de AWS	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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABAC para qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 comprobación de estado de Route 53, consulte [Nombrar y etiquetar las comprobaciones de estado](#) en la Guía para desarrolladores de Amazon Route 53.

[Route53.2] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas 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), .800-53.r5 SI-4 (20), .800-53.r5 SI-7 (8), NIST 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 NIST PCI DSS

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 DNS consultas está habilitado en una zona alojada pública de Amazon Route 53. El control falla si el registro de DNS consultas no está habilitado en una zona alojada pública de Route 53.

El registro de DNS consultas para una zona alojada de Route 53 aborda los requisitos de DNS seguridad y cumplimiento y garantiza la visibilidad. Los registros incluyen información como el dominio o subdominio que se consultó, la fecha y la hora de la consulta, el tipo de DNS registro (por ejemplo, A oAAAA) y el código de DNS respuesta (por ejemplo, NoError oServFail). Cuando

el registro de DNS consultas está habilitado, Route 53 publica los archivos de registro en Amazon CloudWatch Logs.

Corrección

Para registrar DNS las consultas de las zonas alojadas públicas de Route 53, consulte [Configuración del registro de DNS consultas 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 estos controles no estén disponibles en todos 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) 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 v3.2.1/1.3.1, NIST.800-53.r5 SC-7 v3.2.1/1.3.2, v3.2.1/1.3.4, v3.2.1/1.3.4 PCI DSS 1.3,6, PCI DSS PCI DSS PCI DSS PCIDSSv4.0.1/1.4.4

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.

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, 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

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 acceso público a los bloques, la política de depósitos y la lista de control de acceso a los depósitos (ACL). El control lanza un error si el bucket permite el acceso público de lectura.

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) 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 - 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 acceso público a los bloques, la política de depósitos y la lista de control de acceso a los depósitos (ACL). El control lanza un error si el bucket permite el acceso público de escritura.

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] Los depósitos de uso general de S3 deberían requerir solicitudes de uso 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) NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-1 2 (3), NIST.800-53.r5 SC-1 3, 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 (2) NIST.800-53.r5 SC-8, NIST .800-53.r5 SI-7 NIST.800-53.r5 SC-8 (6), v3.2.1/4.1, PCI DSS v4.0.1/4.2.1 PCI DSS

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 solicitudes de usoSSL. El control falla si la política de buckets no requiere solicitudes de usoSSL.

Los buckets de S3 deben tener políticas que exijan que todas las solicitudes (Action: S3:*) solo acepten la transmisión de datos a través HTTPS de la política de recursos de S3, indicada mediante la clave `aws:SecureTransport` de condición.

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 buckets 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

Categoría: Proteger > Gestión del acceso seguro > Operaciones confidenciales restringidas 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, 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 6 (2), (2), NIST .800-53.r5 SI-13 NIST.800-53.r5 SC-5 (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-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) 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), (4), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 v4.0.1/1.4.4 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 PCI DSS

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 (), políticas de depósitos o ambas. ACLs

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), (26), NIST.800-53.r5 AC-4 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, .800-53.r5 SI-4 (20), .800-53.r5 SI-7 (8), NIST v4.0.1/10.2.1 NIST PCI DSS

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 Región de AWS destino debe estar en el 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, .800-53.r5 SI-4, .800-53.r5 SI-4 (4) NIST NIST

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:*, s3:ObjectCreated:CompleteMultipartUpload,	Sin valor predeterminado

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
			s3:ObjectCreated:Copy, s3:ObjectCreated:Post, s3:ObjectCreated:Put, s3:ObjectRemoved:* , s3:ObjectRemoved:Delete, s3:ObjectRemoved:DeleteMarkerCreated , s3:ObjectRestore:* , s3:ObjectRestore:Completed, s3:ObjectRestore:Delete, s3:ObjectRestore:Post,	

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
			s3:ObjectTagging:* , s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReduceRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplication, s3:Replication:OperationMissedThreshold, s3:Replication:OperationNotTracked, s3:Replication:OperationRep	

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
			<p>licatedAfterThreshold, s3:TestEvent</p>	

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 falla si ACL hay una configuración para administrar el acceso de los usuarios al bucket.

ACLs son mecanismos de control de acceso heredados que son anteriores 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 IAM de usuario 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), .800-53.r5 SI-12, NIST .800-53.r5 SI-13 (5) NIST

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: .800-53.r5 CP-6 NIST (2) PCIDSS, 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 S3 Object Lock para cumplir con los requisitos normativos que requieren WORM almacenamiento o añadir un nivel adicional de protección contra los cambios y la eliminación 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, 8, NIST.800-53.r5 SC-2 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), .800-53.r5 AU-9, v4.0.1/3.5.1 NIST PCI DSS

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 falla si el depósito está cifrado con el cifrado predeterminado (SSE-S3).

El cifrado del lado del servidor (SSE) es el cifrado de los datos en su destino por parte de la aplicación o el servicio que los recibe. A menos que especifique lo contrario, los buckets de S3 utilizan las claves gestionadas de Amazon S3 (SSE-S3) de forma predeterminada para el cifrado del lado del servidor. Sin embargo, para un mayor control, puede optar por configurar los buckets para que utilicen el cifrado del lado del servidor con AWS KMS keys (- o -) en su lugar. SSE KMS DSSE KMS 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, 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 (9), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 v4.0.1/1.4.4 PCI DSS

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 cubos de uso general de S3 deberían tener habilitada la función de eliminación 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

AWS Config regla: [s3-bucket-mfa-delete-enabled](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si la eliminación de la autenticación multifactorial (MFA) está habilitada en un bucket versionado de uso general de Amazon S3. El control falla si la MFA eliminación no está habilitada en el bucket. El control no genera resultados para los buckets que tienen una configuración de ciclo de vida.

Al trabajar con el control de versiones de S3 en los buckets de Amazon S3, si lo desea, puede añadir otra capa de seguridad configurando un depósito para permitir MFA la eliminación. Al hacerlo, el propietario del bucket debe incluir dos formas de autenticación en cualquier solicitud para eliminar una versión o cambiar el estado del control de versiones del bucket. MFAeliminar proporciona seguridad adicional si tus credenciales de seguridad se ven comprometidas. MFAeliminar también puede ayudar a evitar que se eliminen bloques accidentalmente, ya que requiere que el usuario

que inicia la acción de eliminación demuestre la posesión física de un MFA dispositivo con un MFA código y añade un nivel adicional de fricción y seguridad a la acción de eliminación.

Note

La función de MFA eliminación requiere el control de versiones en cubos como una dependencia. El control de versiones de buckets es un método para conservar diversas variantes de un objeto de S3 en el mismo bucket. Además, solo el propietario del bucket que haya iniciado sesión como usuario root puede habilitar la MFA eliminación y realizar acciones de eliminación en los buckets de S3.

Corrección

Para habilitar el control de versiones de S3 y configurar la MFA eliminación en un bucket, consulte [Configuración de la MFA eliminación](#) 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, v4.0.1/10.2.1 PCI DSS

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 an 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 ayudarlo a cumplir con los requisitos de conformidad de datos, realizar análisis de seguridad exhaustivos, monitorear patrones específicos de comportamiento de los usuarios en su Cuenta de AWS entorno y tomar medidas en relación con la API actividad a nivel de objeto dentro de sus buckets de S3 mediante Amazon Events. 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, v4.0.1/10.2.1 PCI DSS

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 an 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 ayudarlo a cumplir con los requisitos de conformidad de datos, realizar análisis de seguridad exhaustivos, monitorear patrones específicos de comportamiento de los usuarios en su Cuenta de AWS entorno y tomar medidas en relación con la API actividad a nivel de objeto dentro de sus buckets de S3 mediante Amazon Events. 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: v4.0.1/1.4.4 PCI DSS

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 estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[SageMaker.1] Las instancias de Amazon SageMaker AI 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, 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

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 AI 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, 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 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 AI 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 terminales de SageMaker IA 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`.

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), v4.0.1/8.6.3, PCI DSS v4.0.1/8.3.9 PCI DSS

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
maximumAllowedRotationFrequency	Número máximo de días permitidos para la frecuencia de rotación del secreto	Entero	De 1 a 365	Sin valor predeterminado

Este control comprueba si un secreto almacenado en 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 las credenciales de la base de datos, las contraseñas y API las claves 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 [rotar sus AWS Secrets Manager datos 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), v4.0.1/8.6.3, PCI DSS v4.0.1/8.3.9 PCI DSS

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 las credenciales de la base de datos, las contraseñas y API las claves 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), v4.0.1/8.6.3, PCI DSS v4.0.1/8.3.9 PCI DSS

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	Entero	De 1 a 180	90

Parámetro	Descripción	Tipo	Valores personalizados permitidos	Valor predeterminado de Security Hub
	puede permanecer sin cambios			

Este control comprueba si un AWS Secrets Manager secreto se rota al menos una vez dentro del período de tiempo especificado. 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. Algunos ejemplos son las credenciales de las bases de datos, las contraseñas, API las claves de terceros e incluso el 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
<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	Lista de etiquetas que cumplen los requisitos de AWS	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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para

sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 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 controles de AWS Security Hub evalúan el servicio y los recursos de AWS Service Catalog.

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](#).

[ServiceCatalog.1] Las carteras de Service Catalog solo deben compartirse dentro de una organización de AWS

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 controles de AWS Security Hub 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
<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	Lista de etiquetas que cumplen los requisitos de AWS	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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una lista de contactos de Amazon SES, consulte [TagResource](#) en 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
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	Lista de etiquetas que cumplen los requisitos de AWS	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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a un conjunto de configuración de Amazon SES, consulte [TagResource](#) en 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 de Amazon Simple Notification Service (AmazonSNS).

Es posible que estos controles no estén disponibles en todos Regiones de AWS. Para obtener más información, consulte [Disponibilidad de los controles por región](#).

[SNS.1] SNS los temas 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, 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::SNS::Topic

Regla de AWS Config : [sns-encrypted-kms](#)

Tipo de horario: provocado por un cambio

Parámetros: ninguno

Este control comprueba si un SNS tema de Amazon está cifrado en reposo mediante claves gestionadas en AWS Key Management Service (AWS KMS). Los controles fallan si el SNS tema no usa una KMS clave para el cifrado del lado 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 KMS clave de cifrado en su lugar. 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 API se requieren permisos para descifrar los datos antes de que puedan leerse. Se recomienda cifrar los SNS temas con KMS claves para añadir un nivel de seguridad adicional.

Corrección

Para habilitar un SNS tema, consulte [Habilitar el cifrado del lado del servidor \(SSE\) para un SNS tema de Amazon](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Antes de poder usarlo 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 en los controles de Security Hub](#).

Requisitos relacionados: NIST .800-53.r5 AU-12, .800-53.r5 AU-2 NIST

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 SNS tema de Amazon para los puntos de enlace. 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 SNS punto de conexión de Amazon.
- Identificar la respuesta enviada desde el SNS punto de enlace de Amazon a AmazonSNS.
- Determinar el tiempo de permanencia del mensaje (el tiempo entre la marca de tiempo de publicación y la entrega a un SNS punto final de Amazon).

Corrección

Para configurar el registro del estado de entrega de un tema, consulta el [estado de entrega de los SNS mensajes de Amazon](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

[SNS.3] SNS los temas deben estar etiquetados

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	Lista de etiquetas que cumplen los requisitos de AWS	No default value

Este control comprueba si un SNS tema de Amazon tiene etiquetas con las 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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

 Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 SNS tema, consulte [Configuración de etiquetas de SNS tema de Amazon](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

[SNS.4] las políticas de acceso a los SNS temas 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 SNS temas de Amazon permite el acceso público. Este control falla si la política de acceso a los SNS temas permite el acceso público.

Se utiliza una política de SNS acceso 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). SNSLas políticas pueden conceder acceso a otros Cuentas de AWS usuarios o a usuarios que estén dentro del tuyo Cuenta de AWS. El uso de un carácter comodín (*) en el campo Principle 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.

Corrección

Para actualizar las políticas de acceso de un SNS tema, consulta [Información general sobre la gestión del acceso en Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

Controles de Security Hub para Amazon SQS

Estos controles de AWS Security Hub evalúan el servicio y los recursos de Amazon Simple Queue Service (Amazon SQS).

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](#).

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-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)

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

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. Se produce un error en el control si la cola no está cifrada con una clave administrada por SQS (SSE-SQS) o una clave de AWS Key Management Service (AWS KMS) (SSE-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 servidor (SSE) protege el contenido de los mensajes en las colas de SQS mediante claves de cifrado administradas por SQS (SSE-SQS) o claves de AWS KMS (SSE-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
<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	Lista de etiquetas que cumplen los requisitos de AWS	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.

Las etiquetas se pueden asignar a los recursos de AWS 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 lo 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 recursos de AWS. 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 para permitir 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 conocer más prácticas recomendadas para el etiquetado, consulte [Etiquetado de recursos de AWS](#) en la Referencia general de AWS.

Corrección

Para agregar etiquetas a una cola existente mediante la consola de Amazon SQS, consulte [Configuración de etiquetas de asignación de costos en una cola de Amazon SQS \(consola\)](#) 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 máquina de AWS Step Functions estados 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	Lista de etiquetas que cumplen los requisitos de AWS	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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control

de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni otra información confidencial o delicada 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 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 evalúan el AWS Systems Manager (SSM) 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](#).

[SSM.1] EC2 Las instancias de Amazon deben gestionarse mediante AWS Systems Manager

Requisitos relacionados: PCI DSS v3.2.1/2.4, NIST.800-53.r5 CA-9 (1), 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 (8) NIST.800-53.r5 SA-3, NIST.800-53.r5 SA-1 NIST .800-53.r5 SI-2 (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 están administradas por AWS Systems Manager. Systems Manager es un sistema Servicio de AWS que puede utilizar para ver y controlar su AWS infraestructura.

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 de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche

Requisitos relacionados: NIST .800-53.r5 CM-8 (3), NIST .800-53.r5 SI-2, .800-53.r5 SI-2 (2), NIST .800-53.r5 SI-2 (3), NIST .800-53.r5 SI-2 (5), .800-53.r5 SI-2 (NIST5), v3.2.1/6.2, v4.0.1/2.2.1, NIST v4.0.1/6.3.3 PCI DSS PCI DSS PCI DSS

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.

Al aplicar parches a sus EC2 instancias según lo requiera su organización, se reduce la superficie de ataque 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. Elija 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 de Amazon gestionadas 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, .800-53.r5 CM-2 (2), NIST .800-53.r5 CM-8, .800-53.r5 CM-8 (1), NIST .800-53.r5 CM-8 (3), NIST .800-53.r5 SI-2 (3), NIST v3.2.1/2.4, v4.0.1/2.2.1, v4.0.1/6.3.3 NIST PCI DSS PCI DSS PCI DSS

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 AWS CLI los comandos o API las acciones correspondientes 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. Tras 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] SSM los documentos 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 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 la compartición pública de documentos de Systems Manager, consulte [Bloquear la compartición pública de SSM documentos](#) en la Guía del AWS Systems Manager usuario.

Controles de Security Hub para Transfer Family

Estos AWS Security Hub controles evalúan el AWS Transfer Family 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](#).

[Transfer.1] AWS Transfer Family Los flujos de trabajo 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	Lista de etiquetas que cumplen los requisitos de AWS	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 lo ayuda a realizar un seguimiento de las acciones y las notificaciones de los propietarios responsables de los recursos. Al utilizar el etiquetado, puede implementar el control de acceso basado en atributos (ABAC) como estrategia de autorización, que define los permisos en función de las etiquetas. Puede adjuntar etiquetas a IAM las entidades (usuarios o roles) y a los recursos. AWS Puede crear una ABAC política única o un conjunto de políticas independiente para sus IAM directores. Puede diseñar estas ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso. Para obtener más información, consulte [¿ABACPara qué sirve AWS?](#) en la Guía IAM del usuario.

Note

No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada 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 flujo de trabajo de Transfer Family (consola)

1. Abra la consola. AWS Transfer Family
2. En el panel de navegación, elija Flujos de trabajo. Luego, seleccione el flujo de trabajo que desea etiquetar.
3. Elija Administrar etiquetas y agregue las etiquetas.

[Transfer.2] Los servidores Transfer Family no deben usar el FTP protocolo para la conexión de puntos finales

Requisitos relacionados: NIST.800-53.r5 CM-7, NIST.800-53.r5 IA-5, NIST.800-53.r5 SC-8 v4.0.1/4.2.1 PCI DSS

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 que no sea el de la conexión FTP de punto final. El control falla si el servidor usa el FTP protocolo para que un cliente se conecte al punto final del servidor.

FTP(Protocolo de transferencia de archivos) establece la conexión del punto final a través de canales no cifrados, lo que hace que los datos enviados a través de estos canales sean vulnerables a la interceptación. SSHEl uso de SFTP (protocolo de transferencia de archivos), 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 .

Controles de Security Hub para AWS WAF

Estos AWS Security Hub controles evalúan el AWS WAF 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](#).

[WAF.1] AWS WAF El ACL registro web global clásico 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), v4.0.1/10.4.2 PCI DSS

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 web global. AWS WAF ACL Este control falla si el registro no está habilitado para la webACL.

El registro es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento AWS WAF a nivel mundial. 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 web a la ACL que está conectada AWS WAF.

Corrección

Para habilitar el registro en una AWS WAF webACL, consulte [Registrar la información ACL del tráfico web](#) en la Guía para AWS WAF desarrolladores.

[WAF.2] Las reglas 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 AWS WAF regional tiene al menos una condición. El control falla si no hay condiciones presentes en una regla.

Una regla 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 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 .

[WAF.3] Los grupos de reglas 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 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 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 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 agregar reglas y condiciones de reglas a un grupo de reglas vacío, consulte [Agregar y eliminar reglas de un grupo de reglas AWS WAF clásico](#) y [Agregar y quitar condiciones en una regla](#) en la Guía para AWS WAF desarrolladores.

[WAF.4] La web regional 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 AWS WAF Classic Regional web ACL contiene reglas o grupos de reglas. WAF WAF Este control produce un error si una web ACL no contiene ninguna regla o grupo de WAF reglas.

Una web WAF regional ACL puede contener un conjunto de reglas y grupos de reglas que inspeccionan y controlan las solicitudes web. Si una web ACL está vacía, el tráfico web puede pasar sin que se detecte ni se actúe en consecuencia, WAF según la acción predeterminada.

Corrección

Para añadir reglas o grupos de reglas a una web regional AWS WAF clásica vacíaACL, consulte [Edición de una web ACL](#) en la Guía para AWS WAF desarrolladores.

[WAF.6] Las reglas globales 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 AWS WAF regla global contiene alguna condición. El control falla si no hay condiciones presentes en una regla.

Una regla 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 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 .

[WAF.7] Los grupos de reglas globales 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 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 WAF globales 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 WAF globales 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 AWS WAF clásico](#) en la Guía para AWS WAF desarrolladores.

[WAF.8] La web 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), 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 : :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 web AWS WAF global ACL contiene al menos una WAF WAF regla o un grupo de reglas. El control falla si una web ACL no contiene ninguna regla o grupo de WAF reglas.

Una web WAF global ACL puede contener un conjunto de reglas y grupos de reglas que inspeccionan y controlan las solicitudes web. Si una web ACL está vacía, el tráfico web puede pasar sin que se detecte ni se actúe en consecuencia, WAF según la acción predeterminada.

Corrección

Para añadir reglas o grupos de reglas a una web AWS WAF global vacíaACL, consulte [Edición de una web ACL](#) en la Guía para AWS WAF desarrolladores. Para Filtrar, elija Global (CloudFront).

[WAF.10] la AWS WAF web 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 AWS WAF web (webACL) de la versión 2 contiene al menos una regla o un grupo de reglas. El control falla si una web ACL no contiene ninguna regla o grupo de reglas.

Una web ACL le brinda un control detallado sobre todas las HTTP (S) solicitudes web a las que responde su recurso protegido. Una web ACL debe contener un conjunto de reglas y grupos de reglas que inspeccionen y controlen las solicitudes web. Si una web ACL está vacía, el tráfico web puede pasar sin que se detecte ni se actúe en consecuencia, AWS WAF según la acción predeterminada.

Corrección

Para añadir reglas o grupos de reglas a una WAFV2 web vacíaACL, consulte [Edición de una web ACL](#) en la Guía para AWS WAF desarrolladores.

[WAF.11] El ACL registro AWS WAF web debe estar habilitado

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), (10) 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 (9), NIST .800-53.r5 SI-7 NIST.800-53.r5 SC-7 (8), v4.0.1/10.4.2 PCI DSS

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 (webACL) de la AWS WAF versión 2. Este control falla si el registro está desactivado para la webACL.

Note

Este control no comprueba si el ACL registro AWS WAF web está habilitado para una cuenta a través de Amazon Security Lake.

El registro mantiene la confiabilidad, 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 que analiza tu webACL, puedes solucionar problemas de comportamiento de las aplicaciones.

Corrección

Para activar el registro en una AWS WAF webACL, consulta [Administrar el registro en una web ACL en la Guía para AWS WAF](#) desarrolladores.

[WAF.12] AWS WAF las reglas deben tener las CloudWatch métricas habilitadas

Requisitos relacionados: NIST.800-53.r5 AC-4 (26), (10) 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 SC-7 (9), NIST .800-53.r5 SI-7 (8)

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 tienen habilitadas CloudWatch las métricas de Amazon. El control falla si la regla o el grupo de reglas no tienen CloudWatch las métricas habilitadas.

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 ACL reglas 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 [UpdateRuleGroupAPI](#). Para habilitar CloudWatch las métricas en una AWS WAF regla, invoca la [UpdateWebACLAPI](#). Establezca el campo `CloudWatchMetricsEnabled` como `true`. Al utilizar la AWS WAF consola para crear reglas o grupos de reglas, las CloudWatch métricas se habilitan automáticamente.

Controles de Security Hub para WorkSpaces

Estos controles de AWS Security Hub evalúan el servicio Amazon WorkSpaces y sus 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](#).

[WorkSpaces.1] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

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 usuario en un espacio de trabajo de Amazon WorkSpaces está cifrado en reposo. El control falla si el volumen de usuario de Workspace 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 usuario de WorkSpaces, consulte [Encrypt a Workspace](#) en la Guía de administración de Amazon WorkSpaces.

[WorkSpaces.2] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo

Categoría: Proteger > Protección de datos > Cifrado de datos en reposo

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 en un espacio de trabajo de Amazon WorkSpaces está cifrado en reposo. El control falla si el volumen raíz de Workspace 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 raíz de WorkSpaces, consulte [Encrypt a Workspace](#) en la Guía de administración de Amazon WorkSpaces.

Permisos necesarios para configurar los controles

Para ver información sobre los controles de seguridad y habilitar y deshabilitar los controles de seguridad en los estándares, el rol AWS Identity and Access Management (IAM) al que se accede AWS Security Hub necesita permisos para realizar las siguientes operaciones del Security HubAPI.

Para obtener los permisos necesarios, puede utilizar las [políticas administrada por Security Hub](#). Como alternativa, puede actualizar IAM las políticas 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 de llamada `BatchGetControlEvaluations` a su IAM función. Este permiso es necesario para ver el estado de habilitación y conformidad de un control, el recuento de resultados de los controles y la puntuación de seguridad general de los controles en la consola de Security Hub Como solo se llama a la consola `BatchGetControlEvaluations`, este permiso no corresponde directamente a los AWS CLI comandos APIs ni a los Security Hub documentados públicamente.

Habilitación de controles en Security Hub

En AWS Security Hub, un control es una protección dentro de un estándar de seguridad que ayuda a una organización a proteger la confidencialidad, la integridad y la disponibilidad de la información. Cada control de Security Hub está relacionado con un recurso de AWS específico. Cuando habilita un control, Security Hub comienza a ejecutar controles de seguridad para el control, y a generar resultados para el control. Además, Security Hub tiene en cuenta todos los controles habilitados cuando calcula 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 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 activar y desactivar los controles en cada Región mediante la consola de Security Hub, la API 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 centralizada está disponible para los usuarios que integran Security Hub 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 un control de AWS Security Hub 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 un control de seguridad en varias Cuentas de AWS y Regiones de AWS, debe iniciar sesión en la cuenta de administrador delegado de Security Hub y utilizar la [configuración centralizada](#).

En la configuración centralizada, el administrador delegado puede crear políticas de configuración de Security Hub que habiliten controles específicos en los estándares habilitados. A continuación, puede asociar la política de configuración a cuentas y unidades organizativas (OU) específicas 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 unidad organizativa y puede optar por habilitar solo los controles de Amazon

Elastic Compute Cloud (EC2) 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 habilite controles especificados en estándares, consulte [Creación y asociación de políticas de configuración](#).

Note

El administrador delegado puede crear políticas de configuración para administrar controles en todos los estándares, excepto el [estándar administrado por 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 console

Para habilitar un control en los estándares en una cuenta y región

1. Abra la consola de AWS Security Hub 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 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 los ARN estándar, 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 los ARN estándar, ejecute el comando `describe-standards`.
3. 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"}]'
```

4. Repítalo en cada región en la que quiere habilitar el control.

Habilitación de un control en un estándar específico

Al activar una entrada estándar en AWS Security Hub, todos los controles que se le aplican se habilitan automáticamente en esa norma (con la excepción de los estándares gestionados 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 Cuenta de AWS y 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 en Security Hub](#). Cuando habilita un control en uno o más estándares, Security Hub comienza a generar resultados para ese control. Security Hub 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 de Security Hub en un estándar específico. En lugar de los siguientes pasos, también puedes 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 console

Habilitación de un control en un estándar específico

1. Abra la consola de AWS Security Hub 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 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 los identificadores de control de seguridad independientes del estándar, no los identificadores de control específicos del estándar.

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 los identificadores de control de seguridad independientes del estándar, no los identificadores de control específicos del estándar.

```
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 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 centralizada de Security Hub para habilitar automáticamente los controles nuevos. 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 [Comprensión de la configuración centralizada en Security Hub](#).

Security Hub no habilita los controles nuevos cuando se agregan a un estándar que 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 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 mantendrá esa designación independientemente de si tiene activada la activación automática del control.

Security Hub console

Habilitación automática de nuevos controles

1. Abra la AWS Security Hub consola 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 Guardar.

Security Hub 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](#).

Deshabilitar controles en Security Hub

Existen varias formas de deshabilitar un control en AWS Security Hub. Puede deshabilitar un control en todos los estándares de seguridad o en un estándar específico. Cuando deshabilita un control en todos los estándares, ocurre lo siguiente:

- Los controles de seguridad del control ya no se realizan.
- No se generan hallazgos adicionales para ese control.
- Los resultados existentes se archivan automáticamente después de 3 a 5 días (tenga en cuenta que esto es lo mejor).
- Se quitan las reglas de AWS Config relacionadas que creó Security Hub.

Si deshabilita un control en uno o más de los estándares específicos, Security Hub no ejecuta controles de seguridad para el control de los estándares en los que lo deshabilitó, por lo que no afecta a la puntuación de seguridad de esos estándares. Sin embargo, Security Hub retiene la regla de AWS Config y seguirá ejecutando controles de seguridad para el control si está habilitado en otros estándares. Esto puede afectar a la puntuación de seguridad resumida.

Para reducir el ruido que se produce al detectar ruidos, puede resultar útil deshabilitar los controles que no sean relevantes para su entorno. Para recomendaciones sobre qué controles deshabilitar, consulte [Controles de Security Hub que quizás quiera deshabilitar](#).

Al deshabilitar un estándar, se deshabilitan todos los controles que se le aplican (sin embargo, es posible que esos controles sigan habilitados en otros estándares). Para obtener información acerca de la desactivación de un estándar, consulte [Desactivación de un estándar de seguridad en Security Hub](#).

Cuando deshabilita un estándar, Security Hub no hace un seguimiento de qué controles aplicables se deshabilitaron. Si posteriormente vuelve a habilitar el mismo estándar, todos los controles que se apliquen a ello se habilitarán automáticamente. Además, la desactivación de un control no es una acción permanente. Supongamos que deshabilita un control y, a continuación, habilita un estándar que estaba deshabilitado anteriormente. Si el estándar incluye ese control, se habilitará en ese estándar. Al habilitar un estándar en Security Hub, todos los controles que se aplican a ese estándar se habilitan automáticamente. Puede elegir deshabilitar controles específicos.

Deshabilitar un control en todos los estándares

Recomendamos deshabilitar el control de AWS Security Hub en todos los estándares para mantener la alineación en toda la organización. Si deshabilita un control en estándares específicos, seguirá recibiendo resultados para 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 utilizar una [configuración centralizada](#).

Cuando se utiliza la configuración centralizada, el administrador delegado puede crear políticas de configuración de Security Hub que deshabiliten controles especificados en los estándares habilitados. A continuación, puede asociar la política de configuración a cuentas específicas, unidades organizativas 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 deshabilitar todos los controles de AWS CloudTrail de una unidad organizativa y puede optar por deshabilitar todos los controles de IAM de 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 controles en todos los estándares, excepto el [estándar administrado por 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 seguir estos pasos para deshabilitar un control en una sola cuenta y región.

Security Hub console

Deshabilitación de un control en los estándares en una cuenta y región

1. Abra la consola de AWS Security Hub 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 Deshabilitar 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 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 los ARN estándar, ejecute [DescribeStandards](#).

- 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"}]}
}
```

- 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

- 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
```

- Ejecute el comando [batch-update-standards-control-associations](#). Proporcione el ARN de cualquier estándar en el que esté habilitado el control. Para obtener los ARN estándar, ejecute el comando `describe-standards`.
- 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 en uno o varios estándares específicos de AWS Security Hub. Si el control se aplica a otros estándares habilitados, Security Hub sigue realizando controles de seguridad para el control y genera 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 instrucciones 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 desactivar los controles en los estándares específicos por separado en cada Cuenta de AWS y Región de AWS. Cuando desactiva un control en estándares específicos, solo afecta a la cuenta y a la región actuales.

Elija el método que prefiera y siga los pasos de esta página para deshabilitar un control en uno o varios estándares específicos.

Security Hub console

Deshabilitación de un control en un estándar específico

1. Abra la consola de AWS Security Hub 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 Deshabilitar 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 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 los identificadores de control de seguridad independientes del estándar, no los identificadores de control específicos del estándar.

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 los identificadores de control de seguridad independientes del estándar, no los identificadores de control específicos del estándar.

```
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

Recomendamos desactivar algunos AWS Security Hub controles para reducir la detección de ruido y limitar los costes.

Controles que utilizan recursos globales

Algunos Servicios de AWS admiten recursos globales, lo que significa que puedes acceder al recurso desde cualquier Región de AWS lugar. Para ahorrar costes AWS Config, puedes desactivar el registro de los recursos globales en todas las regiones excepto en una. Una vez hecho esto, Security Hub aún ejecutará controles de seguridad en todas las regiones en las que esté habilitado un control y se le cobrará en función del número de controles por cuenta y región. En consecuencia, para reducir el ruido de resultado y ahorrar en el costo de Security Hub, también debería deshabilitar los controles que incluyen a los 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. Cuando se utiliza 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 el este de EE. UU. (Virginia del Norte)
- GlobalAccelerator.1 — Disponible solo en el oeste de EE. UU. (Oregón)
- Route53.2: disponible solo en la región este de EE. UU. (Norte de Virginia)
- WAF.1, WAF.6, WAF.7 y WAF.8: disponibles solo en la región este de EE. UU. (Norte de Virginia)

Note

Si usa la configuración centralizada, Security Hub deshabilita automáticamente los controles que incluyen 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 los resultados 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 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 [Comprensión de la configuración centralizada en Security Hub](#).

Para los controles con un tipo de programación periódica, es necesario deshabilitarlos en Security Hub para evitar la facturación. Establecer el AWS Config parámetro en `false` no afecta `includeGlobalResourceTypes` a los controles periódicos de Security Hub.

A continuación, se incluye una lista de los controles de Security Hub que utilizan recursos globales:

- [\[Account.1\] La información de contacto de seguridad debe proporcionarse para una Cuenta de AWS](#)
- [\[Account.2\] Cuentas de AWS debe ser parte de una organización de AWS Organizations](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.1\] 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 para los usuarios de IAM deben tener una duración estricta AWS Config](#)
- [\[IAM.11\] 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](#)
- [\[IAM.18\] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte](#)
- [\[IAM.19\] 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 la política adjunta AWSCloud ShellFullAccess](#)
- [\[IAM.28\] El analizador de acceso externo del Analizador de acceso de IAM debe habilitarse](#)
- [\[KMS.1\] 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](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.10\] la AWS WAF web ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado](#)

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 seguimientos en una cuenta de registro centralizada, solo tendrá que habilitar este control en la cuenta y región donde tiene lugar este 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 activado el cifrado en reposo](#)

CloudWatch controles de alarmas

Si prefieres utilizar Amazon GuardDuty para la detección de anomalías en lugar de CloudWatch las alarmas de Amazon, puedes desactivar estos controles, que se centran en CloudWatch las alarmas.

- [\[CloudWatch.1\] Debe existir un filtro de métrica 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 no autorizadas a la API](#)

- [\[CloudWatch.3\] 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](#)
- [\[CloudWatch.5\] Asegúrese de que existan un filtro de métrica de registro y una alarma para los cambios de duración de CloudTrail de AWS Config](#)
- [\[CloudWatch.6\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los errores de autenticación de AWS Management Console](#)
- [\[CloudWatch.7\] 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 bucket S3](#)
- [\[CloudWatch.9\] Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios de configuración de AWS Config](#)
- [\[CloudWatch.10\] 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](#)

Descripción de los controles y las puntuaciones de seguridad

AWS Security Hub Ejecuta comprobaciones de seguridad para cada control que active. 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 [Activación y configuración AWS Config de Security Hub](#). Para obtener una lista de AWS Config los recursos que debe registrar para cada norma, consulte [AWS Config Recursos necesarios para las conclusiones sobre el control de Security Hub](#). Otros controles utilizan funciones Lambda personalizadas, que son administradas por Security Hub y no requieren ningún requisito previo.

A medida que Security Hub ejecuta los controles de seguridad, genera resultados y les asigna un estado de conformidad. Para obtener más información sobre el estado de conformidad, consulte [Evaluación del estado de conformidad de los resultados de Security Hub](#).

Security Hub utiliza el estado de conformidad de los resultados de control para determinar un estado de control general. En función del estado de control, Security Hub también calcula una puntuación de seguridad en 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 resultados de control consolidados, Security Hub genera un único resultado 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 las conclusiones sobre el control de Security Hub](#)
- [Programación para ejecutar comprobaciones de seguridad](#)
- [Generación y actualización de los resultados de control](#)
- [Evaluación del estado de control y el estado de conformidad en Security Hub](#)
- [Calcular las puntuaciones de seguridad](#)

AWS Config Recursos necesarios para las conclusiones sobre el control de Security Hub

Algunos AWS Security Hub controles utilizan AWS Config reglas vinculadas a servicios que detectan los cambios de configuración AWS en los recursos. Para que Security Hub genere resultados de control precisos, debe habilitar AWS Config y activar el registro de recursos AWS Config. Para

obtener un contexto sobre cómo Security Hub usa AWS Config las reglas y cómo habilitarlas y AWS Config configurarlas, consulte [Activación y configuración AWS Config de Security Hub](#).

Para recibir 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 cada control de Security Hub.

Los controles de Security Hub pueden basarse en AWS Config reglas administradas o reglas de Security Hub personalizadas. Asegúrese de que no haya ninguna política AWS Identity and Access Management (de IAM) o una política gestionada en Organizations que AWS Config impida tener permiso para registrar sus recursos. Las comprobaciones de control de Security Hub evalúan directamente la configuración de un recurso y no tienen en cuenta las políticas de Organizations. Para obtener más información sobre el AWS Config registro, consulte [la Lista de reglas AWS Config administradas: consideraciones](#) en la Guía para AWS Config desarrolladores.

Note

Si Regiones de AWS un control no está disponible, el recurso correspondiente no está disponible en AWS Config. Para obtener una lista de los límites Regionales de los controles de Security Hub, consulte [Límites regionales para los controles de Security Hub](#).

Recursos necesarios para todos los controles de Security Hub

Para que Security Hub genere resultados sobre los controles activados por cambios en el Security Hub habilitados que utilizan una AWS Config regla, debe registrar estos recursos en AWS Config. En esta tabla también se indican los controles que evalúan un recurso concreto. Un único control puede evaluar más de un recurso.

Servicio	Recursos necesarios	Controles relacionados
Amazon API Gateway	AWS::ApiGateway::Stage	APIGateway1. APIGateway2. APIGateway3. APIGateway4.

Servicio	Recursos necesarios	Controles relacionados
		APIGateway5.
	AWS::ApiGatewayV2:Stage	APIGateway1. APIGateway9.
AWS AppConfig	AWS::AppConfig::Application	AppConfig1.
	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.

Servicio	Recursos necesarios	Controles relacionados
AWS AppSync	AWS::AppSync::GraphQLApi	AppSync2. AppSync4. AppSync5.
	AWS::AppSync::ApiCache	AppSync1. AppSync6.
AWS Backup (AWS Backup)	AWS::Backup::BackupPlan	Backup.5
	AWS::Backup::BackupVault	Backup.3
	AWS::Backup::RecoveryPoint	Backup.1 Backup.2
	AWS::Backup::ReportPlan	Backup.4
AWS Batch	AWS::Batch::ComputeEnvironment	Lote 3
	AWS::Batch::JobQueue	Lote.1
	AWS::Batch::SchedulingPolicy	Lote.2

Servicio	Recursos necesarios	Controles relacionados
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
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

Servicio	Recursos necesarios	Controles relacionados
AWS CloudTrail	AWS::CloudTrail::Trail	CloudTrail9.
Amazon CloudWatch	AWS::CloudWatch::Alarm	CloudWatch.15 CloudWatch.17
AWS CodeArtifact	AWS::CodeArtifact::Repository	CodeArtifact1.
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

Servicio	Recursos necesarios	Controles relacionados
Amazon Cognito	AWS::Cognito::UserPool	Cognito.1
Amazon Connect	AWS::CustomerProfiles::ObjectType	Conectar.1
AWS DataSync	AWS::DataSync::Task	DataSync1.
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	

Servicio	Recursos necesarios	Controles relacionados
	AWS::DMS: :ReplicationTask	DMS.7 DMS.8
Amazon DynamoDB	AWS::DynamoDB::Table	DynamoDB.1 DynamoDB.2 DynamoDB.5 DynamoDB.6
Amazon Elastic Compute Cloud (EC2)	AWS::EC2: :ClientVpnEndpoint	EC25.1
	AWS::EC2: :CustomerGateway	EC2.36
	AWS::EC2::EIP	EC2.12 EC2.37
	AWS::EC2: :FlowLog	EC2.48

Servicio	Recursos necesarios	Controles relacionados
	AWS::EC2: :Instance	EC24. EC2.8. EC2.9. EC2.17 EC2.24 EC2.38 EMR.1 SSM.1
	AWS::EC2: :Internet Gateway	EC2.39
	AWS::EC2: :LaunchTe mplate	EC2.25 EC2.170
	AWS::EC2: :NatGateway	EC2.40
	AWS::EC2: :NetworkAc1	EC2.16 EC2.21 EC2.41
	AWS::EC2: :NetworkI nterface	EC2.22 EC2.35
	AWS::EC2: :RouteTable	EC2.42

Servicio	Recursos necesarios	Controles relacionados
	AWS::EC2: :SecurityGroup	EC22. EC2.13 EC2.14 EC2.18 EC2.19 EC2.43
	AWS::EC2: :Subnet	EC2.15 EC2.44 ElastiCache.7.
	AWS::EC2: :TransitG ateway	EC2.23 EC2.52
	AWS::EC2: :TransitG atewayAtt achment	EC2.33
	AWS::EC2: :TransitG atewayRou teTable	EC2.34
	AWS::EC2: :Volume	EC23. EC2.45
	AWS::EC2::VPC	EC2.6. EC2.46

Servicio	Recursos necesarios	Controles relacionados
	AWS::EC2: :VPCBlock PublicAcc essOptions	EC2.172
	AWS::EC2: :VPCEndpo intService	EC2.47
	AWS::EC2: :VPCPeeri ngConnection	EC2.49
	AWS::EC2: :VPNConnection	EC2.20 EC2.171
	AWS::EC2: :VPNGateway	EC2.50
Amazon EC2 Auto Scaling	AWS::Auto Scaling:: AutoScali ngGroup	AutoScaling1. AutoScaling2. AutoScaling6. AutoScaling.9. AutoScaling.10
	AWS::Auto Scaling:: LaunchCon figuration	AutoScaling3. Autoscaling.5
Amazon EC2 Systems Manager (SSM)	AWS::SSM: :Associat ionCompliance	SSM.3

Servicio	Recursos necesarios	Controles relacionados
	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
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS: :Cluster	EC.12 ECS.14
	AWS::ECS: :Service	ECS.2 ECS.10 ECS.13

Servicio	Recursos necesarios	Controles relacionados
	AWS::ECS: :TaskDefinition	ECS.1 ECS.3 ECS.4 ECS.5 ECS.8 ECS.9 ECS.15
	AWS::ECS: :TaskSet	ECS.16
Amazon Elastic File System (Amazon EFS)	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	Recursos necesarios	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::LoadBalancer	ELB.1 ELB.4 ELB.5 ELB.6 ELB.12 ELB.13 ELB.16

Servicio	Recursos necesarios	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	Recursos necesarios	Controles relacionados
	AWS::FraudDetector::Variable	FraudDetector4.
AWS Global Accelerator	AWS::GlobalAccelerator::Accelerator	GlobalAccelerator1.
AWS Glue	AWS::Glue::Job	Glue.1
	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	Recursos necesarios	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	Recursos necesarios	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< td=""> <td>IoT TEvents 1.3</td> </alarmmodel<>	IoT TEvents 1.3
	AWS::IoTEvents:: <detectormodel< td=""> <td>IoT TEvents 3.2</td> </detectormodel<>	IoT TEvents 3.2
	AWS::IoTEvents:: <input< td=""> <td>IoT TEvents 1.1</td> </input<>	IoT TEvents 1.1
AWS Eventos de IoT	AWS::IoTEvents:: <alarmmodel< td=""> <td>IoT TEvents 1.3</td> </alarmmodel<>	IoT TEvents 1.3

Servicio	Recursos necesarios	Controles relacionados
	AWS::IoTEvents::DetectorModel	IoTEvents 3.2
	AWS::IoTEvents::Input	IoTEvents 1.1
AWS IoT SiteWise	AWS::IoTSiteWise::AssetModel	IoTSiteWise.1
	AWS::IoTSiteWise::Dashboard	IoTSiteWise.2
	AWS::IoTSiteWise::Gateway	IoTSiteWise.3
	AWS::IoTSiteWise::Portal	IoTSiteWise.4
	AWS::IoTSiteWise::Project	IoTSiteWise.5
AWS IoT TwinMaker	AWS::IoT TwinMaker::Entity	IoT TwinMaker.4
	AWS::IoT TwinMaker::Scene	IoT TwinMaker.3

Servicio	Recursos necesarios	Controles relacionados
	AWS::IoTwinMaker:SyncJob	Io Maker.1 TTwin
	AWS::IoTwinMaker:Workspace	Io Maker.2 TTwin
AWS IoT Wireless	AWS::IoTWireless:MulticastGroup	Io TWireless 1.1
	AWS::IoTWireless:ServiceProfile	Io TWireless 1.2
	AWS::IoTWireless:FuotaTask	Io TWireless 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

Servicio	Recursos necesarios	Controles relacionados
AWS Lambda	AWS::Lambda::Function	Lambda.1 Lambda.2 Lambda.3 Lambda.5 Lambda.6
Amazon MSK	AWS::MSK::Cluster	MSK.1 MSK.2
	AWS::KafkaConnect::Connector	MSK.3
Amazon MQ	AWS::AmazonMQ::Broker	MQ.2 MQ.3 MQ.4 MQ.5 MQ.6
AWS Network Firewall	AWS::NetworkFirewall::Firewall	NetworkFirewall1. NetworkFirewall7. NetworkFirewall.9.

Servicio	Recursos necesarios	Controles relacionados
	AWS::NetworkFirewall::FirewallPolicy	NetworkFirewall3. NetworkFirewall4. NetworkFirewall5. NetworkFirewall.8.
	AWS::NetworkFirewall::RuleGroup	NetworkFirewall6.
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	Recursos necesarios	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	Recursos necesarios	Controles relacionados
	AWS::RDS::DBClusterSnapshot	RDS.37 DocumentDB.3 Neptune.3 Neptune.6 RDS.1 RDS.4 RDS.29

Servicio	Recursos necesarios	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
	AWS::RDS: :DBSecurityGroup	RDS.31
	AWS::RDS: :DBSnapshot	RDS.1 RDS.4 RDS.32

Servicio	Recursos necesarios	Controles relacionados
	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
	AWS::Redshift::ClusterParameterGroup	Redshift.2
	AWS::Redshift::ClusterSnapshot	Redshift.13

Servicio	Recursos necesarios	Controles relacionados
	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	Recursos necesarios	Controles relacionados
	AWS::S3::Bucket	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
Amazon SageMaker AI	AWS::SageMaker::NotebookInstance	SageMaker2. SageMaker3.
	AWS::SageMaker::Model	SageMaker5.

Servicio	Recursos necesarios	Controles relacionados
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
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue	SQS.1 SQS.2
AWS Step Functions	AWS::StepFunctions::StateMachine	StepFunctions1.
	AWS::StepFunctions::Activity	StepFunctions2.
AWS Transfer Family	AWS::Transfer::Workflow	Transfer.1

Servicio	Recursos necesarios	Controles relacionados
AWS WAF	AWS::WAF::Rule	WAF.6
	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 FSBP

Para que Security Hub informe con precisión de las conclusiones de los controles activados por cambios de AWS Foundational Security Best Practices v1.0.0 (FSBP) que utilizan una AWS Config regla, debe registrar estos recursos en AWS Config. Para obtener más información sobre este estándar, consulte [AWS Estándar básico de mejores prácticas de seguridad v1.0.0 \(FSBP\)](#).

Servicio	Recursos necesarios de
Amazon API Gateway	AWS::ApiGateway::Stage AWS::ApiGatewayV2::Stage
AWS AppSync	AWS::AppSync::ApiCache 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
AWS CodeBuild	AWS::CodeBuild::Project AWS::CodeBuild::ReportGroup
Amazon Cognito	AWS::Cognito::UserPool
AWS DataSync	AWS::DataSync::Task
AWS Database Migration Service (AWS DMS)	AWS::DMS::Endpoint AWS::DMS::ReplicationInstance AWS::DMS::ReplicationTask
Amazon DynamoDB	AWS::DynamoDB::Table
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance AWS::SSM::ManagedInstanceInventory AWS::SSM::PatchCompliance
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::ClientVpnEndpoint

Servicio	Recursos necesarios de
	<p>AWS::EC2::Instance</p> <p>AWS::EC2::LaunchTemplate</p> <p>AWS::EC2::NetworkAcl</p> <p>AWS::EC2::NetworkInterface</p> <p>AWS::EC2::SecurityGroup</p> <p>AWS::EC2::Subnet</p> <p>AWS::EC2::TransitGateway</p> <p>AWS::EC2::VPCLockPublicAccessOptions</p> <p>AWS::EC2::VPNConnection</p> <p>AWS::EC2::Volume</p>
Amazon EC2 Auto Scaling	<p>AWS::AutoScaling::AutoScalingGroup</p> <p>AWS::AutoScaling::LaunchConfiguration</p>
Amazon Elastic Container Registry (Amazon ECR)	<p>AWS::ECR::Repository</p>
Amazon Elastic Container Service (Amazon ECS)	<p>AWS::ECS::Cluster</p> <p>AWS::ECS::Service</p> <p>AWS::ECS::TaskDefinition</p> <p>AWS::ECS::TaskSet</p>

Servicio	Recursos necesarios de
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint AWS::EFS::FileSystem
Amazon EKS	AWS::EKS::Cluster
ElasticBeanstalk	AWS::ElasticBeanstalk::Environment
Elastic Load Balancing	AWS::ElasticLoadBalancing::LoadBalancer AWS::ElasticLoadBalancingV2::LoadBalancer
ElasticSearch	AWS::Elasticsearch::Domain
Amazon EMR	AWS::EMR::SecurityConfiguration
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 MSK	AWS::MSK::Cluster AWS::KafkaConnect::Connector

Servicio	Recursos necesarios de
AWS Network Firewall	<p>AWS::NetworkFirewall::Firewall</p> <p>AWS::NetworkFirewall::FirewallPolicy</p> <p>AWS::NetworkFirewall::RuleGroup</p>
OpenSearch Servicio Amazon	AWS::OpenSearch::Domain
Amazon Relational Database Service (Amazon RDS)	<p>AWS::RDS::DBCluster</p> <p>AWS::RDS::DBClusterSnapshot</p> <p>AWS::RDS::DBInstance</p> <p>AWS::RDS::DBSnapshot</p> <p>AWS::RDS::EventSubscription</p>
Amazon Redshift	<p>AWS::Redshift::Cluster</p> <p>AWS::Redshift::ClusterSubnetGroup</p>
Amazon Route 53	AWS::Route53::HostedZone
Amazon Simple Storage Service (Amazon S3)	<p>AWS::S3::AccessPoint</p> <p>AWS::S3::AccountPublicAccessBlock</p> <p>AWS::S3::Bucket</p> <p>AWS::S3::MultiRegionAccessPoint</p>
Amazon SageMaker AI	<p>AWS::SageMaker::Model</p> <p>AWS::SageMaker::NotebookInstance</p>

Servicio	Recursos necesarios de
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue
AWS Secrets Manager	AWS::SecretsManager::Secret
AWS Step Functions	AWS::StepFunctions::StateMachine
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
Amazon WorkSpaces	AWS::WorkSpaces::Workspace

Recursos necesarios para CIS AWS Foundations Benchmark

Para ejecutar comprobaciones de seguridad para los controles habilitados que se aplican al punto de referencia fundamental del Center for Internet Security (CIS) AWS , Security Hub sigue los pasos de auditoría exactos prescritos para las comprobaciones en [Securing Amazon Web Services](#) o utiliza reglas AWS Config gestionadas específicas.

Para obtener más información sobre este estándar, consulte [Indicador de referencia de CIS AWS Foundations](#).

Recursos necesarios para CIS v3.0.0

Para que Security Hub 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 estos recursos en. AWS Config

Servicio	Recursos necesarios de
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::Instance AWS::EC2::NetworkACL AWS::EC2::SecurityGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Group AWS::IAM::User AWS::IAM::Role
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBInstance
Amazon Simple Storage Service (Amazon S3)	AWS::S3::Bucket

Recursos de necesarios para CIS v1.4.0

Para que Security Hub 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 estos recursos en. AWS Config

Servicio	Recursos necesarios de
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::NetworkACL AWS::EC2::SecurityGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Policy AWS::IAM::User

Servicio	Recursos necesarios de
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBInstance
Amazon Simple Storage Service (Amazon S3)	AWS::S3::Bucket

Recursos de necesarios para CIS v1.2.0

Para que Security Hub 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 estos recursos en. AWS Config

Servicio	Recursos necesarios de
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::SecurityGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Policy AWS::IAM::User

Recursos necesarios para NIST SP 800-53 Rev. 5

Para que Security Hub informe con precisión las conclusiones de los controles activados por cambios SP 800-53 Rev. 5 del Instituto Nacional de Estándares y Tecnología (NIST) que utilizan una AWS Config regla, debe registrar estos recursos en. AWS Config Solo tiene que registrar los recursos de los controles en los que se haya activado un cambio de tipo programado. Para obtener más información sobre este estándar, consulte [NIST SP 800-53 Rev. 5 en Security Hub](#).

Servicio	Recursos necesarios de
Amazon API Gateway	AWS::ApiGateway::Stage AWS::ApiGatewayV2::Stage
AWS AppSync	AWS::AppSync::GraphQLApi
AWS Backup	AWS::Backup::RecoveryPoint

Servicio	Recursos necesarios de
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
AWS Database Migration Service (AWS DMS)	AWS::DMS::Endpoint AWS::DMS::ReplicationInstance AWS::DMS::ReplicationTask
Amazon DynamoDB	AWS::DynamoDB::Table
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::ClientVpnEndpoint AWS::EC2::EIP AWS::EC2::Instance AWS::EC2::LaunchTemplate AWS::EC2::NetworkAcl AWS::EC2::NetworkInterface AWS::EC2::SecurityGroup AWS::EC2::Subnet AWS::EC2::TransitGateway AWS::EC2::VPNConnection AWS::EC2::Volume

Servicio	Recursos necesarios de
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
Amazon EMR	AWS::EMR::SecurityConfiguration
Amazon EventBridge	AWS::Events::Endpoint AWS::Events::EventBus

Servicio	Recursos necesarios de
AWS Identity and Access Management (IAM)	<p>AWS::IAM::Group</p> <p>AWS::IAM::Policy</p> <p>AWS::IAM::Role</p> <p>AWS::IAM::User</p>
AWS Key Management Service (AWS KMS)	<p>AWS::KMS::Alias</p> <p>AWS::KMS::Key</p>
Amazon Kinesis	AWS::Kinesis::Stream
AWS Lambda	AWS::Lambda::Function
Amazon MSK	AWS::MSK::Cluster
Amazon MQ	AWS::AmazonMQ::Broker
AWS Network Firewall	<p>AWS::NetworkFirewall::Firewall</p> <p>AWS::NetworkFirewall::FirewallPolicy</p> <p>AWS::NetworkFirewall::RuleGroup</p>
OpenSearch Servicio Amazon	AWS::OpenSearch::Domain
Amazon Relational Database Service (Amazon RDS)	<p>AWS::RDS::DBCluster</p> <p>AWS::RDS::DBClusterSnapshot</p> <p>AWS::RDS::DBInstance</p> <p>AWS::RDS::DBSnapshot</p> <p>AWS::RDS::EventSubscription</p>

Servicio	Recursos necesarios de
Amazon Redshift	AWS::Redshift::Cluster AWS::Redshift::ClusterSubnetGroup
Amazon Route 53	AWS::Route53::HostedZone
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccountPublicAccessBlock AWS::S3::AccessPoint AWS::S3::Bucket
AWS Service Catalog	AWS::ServiceCatalog::Portfolio
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance AWS::SSM::ManagedInstanceInventory AWS::SSM::PatchCompliance
Amazon SageMaker AI	AWS::SageMaker::NotebookInstance
AWS Secrets Manager	AWS::SecretsManager::Secret

Servicio	Recursos necesarios de
AWS WAF	<p>AWS::WAF::Rule</p> <p>AWS::WAF::RuleGroup</p> <p>AWS::WAF::WebACL</p> <p>AWS::WAFRegional::Rule</p> <p>AWS::WAFRegional::RuleGroup</p> <p>AWS::WAFRegional::WebACL</p> <p>AWS::WAFv2::RuleGroup</p> <p>AWS::WAFv2::WebACL</p>

Recursos necesarios para PCI DSS v3.2.1

Para que Security Hub informe con precisión de las conclusiones de los controles del Estándar de Seguridad de Datos del Sector de Tarjetas de Pago (PCI DSS) habilitados que utilizan una AWS Config regla, debe registrar estos recursos en. AWS Config Para obtener más información sobre este estándar, consulte [PCI DSS en Security Hub](#).

Servicio	Recursos necesarios de
AWS CodeBuild	AWS::CodeBuild::Project
Amazon Elastic Compute Cloud (EC2)	<p>AWS::EC2::EIP</p> <p>AWS::EC2::Instance</p> <p>AWS::EC2::SecurityGroup</p>
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Policy

Servicio	Recursos necesarios de
	AWS::IAM::User
AWS Lambda	AWS::Lambda::Function
OpenSearch Servicio Amazon	AWS::OpenSearch::Domain
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBClusterSnapshot AWS::RDS::DBInstance AWS::RDS::DBSnapshot
Amazon Redshift	AWS::Redshift::Cluster
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccountPublicAccessBlock AWS::S3::Bucket
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance AWS::SSM::ManagedInstanceInventory AWS::SSM::PatchCompliance

Recursos necesarios para el estándar de etiquetado AWS de recursos

Todos los controles del estándar AWS de etiquetado de recursos se activan mediante cambios y utilizan una AWS Config regla. Para que Security Hub informe con precisión de los hallazgos de estos controles, debe registrar los siguientes recursos en AWS Config. Para obtener más información sobre este estándar, consulte [AWS Estándar de etiquetado de recursos](#).

Servicio	Recursos necesarios de
AWS AppConfig	AWS::AppConfig::Application

Servicio	Recursos necesarios de
	AWS::AppConfig::Configurati onProfile AWS::AppConfig::Environment AWS::AppConfig::ExtensionAs sociation
Amazon AppFlow	AWS::AppFlow::Flow
AWS App Runner	AWS::AppRunner::Service AWS::AppRunner::VpcConnector
AWS AppSync	AWS::AppSync::GraphQLApi
Amazon Athena	AWS::Athena::DataCatalog AWS::Athena::WorkGroup
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS Backup (AWS Backup)	AWS::Backup::BackupPlan AWS::Backup::BackupVault AWS::Backup::RecoveryPlan AWS::Backup::ReportPlan
AWS Batch	AWS::Batch::ComputeEnvironment AWS::Batch::JobQueue AWS::Batch::SchedulingPolicy
AWS CloudFormation	AWS::CloudFormation::Stack
Amazon CloudFront	AWS::CloudFront::Distribution

Servicio	Recursos necesarios de
AWS CloudTrail	AWS::CloudTrail::Trail
AWS CodeArtifact	AWS::CodeArtifact::Repository
Amazon CodeGuru	AWS::CodeGuruProfiler::ProfilingGroup AWS::CodeGuruReviewer::RepositoryAssociation
Amazon Connect	AWS::CustomerProfiles::ObjectType
Amazon Detective	AWS::Detective::Graph
AWS Database Migration Service (AWS DMS)	AWS::DMS::Certificate AWS::DMS::EventSubscription AWS::DMS::ReplicationInstance AWS::DMS::ReplicationSubnetGroup
Amazon DynamoDB	AWS::DynamoDB::Trail

Servicio	Recursos necesarios de
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::CustomerGateway AWS::EC2::EIP AWS::EC2::FlowLog AWS::EC2::Instance AWS::EC2::InternetGateway AWS::EC2::NatGateway AWS::EC2::NetworkAcl AWS::EC2::NetworkInterface AWS::EC2::RouteTable AWS::EC2::SecurityGroup AWS::EC2::Subnet 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	Recursos necesarios de
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 (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>

Servicio	Recursos necesarios de
Amazon GuardDuty	AWS::GuardDuty::Detector AWS::GuardDuty::Filter AWS::GuardDuty::IPSet
AWS Identity and Access Management (IAM)	AWS::IAM::Role AWS::IAM::User
AWS Identity and Access Management Access Analyzer (Analizador de acceso IAM)	AWS::AccessAnalyzer::Analyzer
AWS IoT	AWS::IoT::Authorizer AWS::IoT::Dimension AWS::IoT::MitigationAction AWS::IoT::Policy AWS::IoT::RoleAlias AWS::IoT::SecurityProfile
AWS IoT Eventos	AWS::IoTEvents::AlarmModel AWS::IoTEvents::DetectorModel AWS::IoTEvents::Input
AWS IoT SiteWise	AWS::IoTSiteWise::Dashboard AWS::IoTSiteWise::Gateway AWS::IoTSiteWise::Portal AWS::IoTSiteWise::Project

Servicio	Recursos necesarios de
AWS IoT TwinMaker	<p>AWS::IoT::TwinMaker::Entity</p> <p>AWS::IoT::TwinMaker::Scene</p> <p>AWS::IoT::TwinMaker::SyncJob</p> <p>AWS::IoT::TwinMaker::Workspace</p>
AWS IoT Conexión inalámbrica	<p>AWS::IoTWireless::FuotaTask</p> <p>AWS::IoTWireless::MulticastGroup</p> <p>AWS::IoTWireless::ServiceProfile</p>
Amazon Interactive Video Service (Amazon IVS)	<p>AWS::IVS::Channel</p> <p>AWS::IVS::PlaybackKeyPair</p> <p>AWS::IVS::RecordingConfiguration</p>
Amazon Keyspaces (para Apache Cassandra)	AWS::Cassandra::Keyspace
Amazon Kinesis	AWS::Kinesis::Stream
AWS Lambda	AWS::Lambda::Function
Amazon MQ	AWS::AmazonMQ::Broker
AWS Network Firewall	<p>AWS::NetworkFirewall::Firewall</p> <p>AWS::NetworkFirewall::FirewallPolicy</p>
OpenSearch Servicio Amazon	AWS::OpenSearch::Domain
AWS Private Certificate Authority	AWS::ACMPCA::CertificateAuthority

Servicio	Recursos necesarios de
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::ClusterSnapshot AWS::Redshift::ClusterSubnetGroup AWS::Redshift::EventSubscription
Amazon Route 53	AWS::Route53::HealthCheck
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
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue
AWS Step Functions	AWS::StepFunctions::Activity
AWS Transfer Family	AWS::Transfer::Workflow

Recursos necesarios para el estándar gestionado por servicios: AWS Control Tower

Para que Security Hub informe con precisión de las conclusiones de los controles activados por Service-Managed Standard: AWS Control Tower change activados que utilizan una AWS Config regla, debe registrar los siguientes recursos en. AWS Config Para obtener más información sobre este estándar, consulte [Estándar de gestión de servicios: AWS Control Tower](#).

Servicio	Recursos necesarios de
Amazon API Gateway	AWS::ApiGateway::Stage AWS::ApiGatewayV2::Stage
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS CodeBuild	AWS::CodeBuild::Project
Amazon DynamoDB	AWS::DynamoDB::Table
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::Instance AWS::EC2::NetworkAcl AWS::EC2::NetworkInterface 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

Servicio	Recursos necesarios de
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
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

Servicio	Recursos necesarios de
AWS Network Firewall	<p>AWS::NetworkFirewall::FirewallPolicy</p> <p>AWS::NetworkFirewall::RuleGroup</p>
OpenSearch Servicio Amazon	AWS::OpenSearch::Domain
Amazon Relational Database Service (Amazon RDS)	<p>AWS::RDS::DBCluster</p> <p>AWS::RDS::DBClusterSnapshot</p> <p>AWS::RDS::DBInstance</p> <p>AWS::RDS::DBSnapshot</p> <p>AWS::RDS::EventSubscription</p>
Amazon Redshift	AWS::Redshift::Cluster
Amazon Simple Storage Service (Amazon S3)	<p>AWS::S3::AccountPublicAccessBlock</p> <p>AWS::S3::Bucket</p>
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue
Amazon EC2 Systems Manager (SSM)	<p>AWS::SSM::AssociationCompliance</p> <p>AWS::SSM::ManagedInstanceInventory</p> <p>AWS::SSM::PatchCompliance</p>
AWS Secrets Manager	AWS::SecretsManager::Secret

Servicio	Recursos necesarios de
AWS WAF	AWS::WAFRegional::Rule AWS::WAFRegional::RuleGroup AWS::WAFRegional::WebACL AWS::WAFv2::WebACL

Programación para ejecutar comprobaciones de seguridad

Después de habilitar un estándar de seguridad, AWS Security Hub comienza a ejecutar todas las comprobaciones en el plazo de dos horas. La mayoría de las comprobaciones comienzan a ejecutarse en 25 minutos. Security Hub 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 puede tardar hasta 24 horas en generar resultados para los controles que utilizan la misma regla subyacente de AWS Config vinculada a servicios que los controles habilitados de otros estándares habilitados. Por ejemplo, si habilita [Lambda.1](#) en el estándar AWS Foundational Security Best Practices (FSBP), Security Hub creará la regla vinculada al servicio y, por lo general, generará resultados en cuestión de minutos. Después de esto, si habilita Lambda.1 en el Estándar de seguridad de datos del sector de tarjetas de pago (PCI DSS), Security Hub puede tardar hasta 24 horas en generar resultados para este control, ya que utiliza la misma regla vinculada a servicios que Lambda.1.

Después de la comprobación inicial, la programación de cada control puede ser periódica o activada por cambios. Para un control basado en una regla de AWS Config administrada, la descripción del control incluye un enlace a la descripción de la regla en la AWS Config Guía del desarrollador. Esa descripción incluye si la regla está activada 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 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 el resultado de KMS.4: la rotación de AWS KMS key debe estar habilitada y, a continuación, corregir el resultado), Security Hub cambia el estado del flujo de trabajo de NEW a 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 de Lambda personalizadas de Security Hub son periódicas.

Controles de seguridad desencadenados por cambios

Los controles de seguridad desencadenados por cambios se ejecutan cuando el recurso asociado cambia de estado. AWS Config 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 periodo de 24 horas si se producen cambios en el estado de dichos recursos. Si no hay cambios, no se entrega ningún dato. Esto puede retrasar la generación de los resultados de Security Hub hasta que se complete un periodo de 24 horas. Independientemente del periodo de registro que haya elegido, Security Hub lo comprueba cada 18 horas para garantizar que no se haya omitido ninguna actualización de recursos de AWS Config.

En general, Security Hub utiliza reglas activadas por cambios siempre que sea posible. Para que un recurso utilice una regla activada por cambios, debe haber compatibilidad con elementos de configuración de AWS Config.

Generación y actualización de los resultados de control

AWS Security Hub genera resultados mediante la realización de comprobaciones comparándolas con los controles de seguridad. Estos hallazgos utilizan el formato AWS de búsqueda de seguridad (ASFF). Tenga en cuenta que si el tamaño del resultado supera el máximo de 240 KB, se eliminará el objeto `Resource.Details`. En el caso de los controles respaldados por AWS Config recursos, puede ver los detalles de los recursos en la AWS Config consola.

Security Hub normalmente cobra por cada control de seguridad de un control. Sin embargo, si varios controles utilizan la misma AWS Config regla, Security Hub solo cobrará una vez por cada comprobación según la AWS Config regla. Si habilita los [resultados de control consolidados](#), Security Hub genera un único resultado para un control de seguridad, incluso cuando el control está incluido en varios estándares habilitados.

Por ejemplo, varios controles utilizan la AWS Config regla `iam-password-policy` en el estándar Center for Internet Security (CIS) AWS Foundations Benchmark y en el estándar Foundational Security Best Practices. Cada vez que Security Hub comprueba el cumplimiento de esa AWS Config regla, genera una comprobación independiente para cada control relacionado, pero solo cobra una vez por la comprobación.

Resultados de control consolidados

Si los hallazgos de control consolidados están habilitados en su cuenta, Security Hub 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 ver una lista de los controles y los estándares a los que se aplican, consulte [Referencia de controles de Security Hub](#). Recomendamos habilitar los resultados de control consolidados para reducir el ruido de resultados.


Si habilitó 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 habilita Security Hub el 23 de febrero de 2023 o después, los resultados de control consolidados se habilitarán de manera automática en su cuenta. Sin embargo, si utiliza la [integración de Security Hub con AWS Organizations](#) o invitó a cuentas de miembro mediante un [proceso de invitación manual](#), los resultados de control consolidados solo se habilitarán en las cuentas de miembro si están habilitados en la cuenta de administrador. Si la característica está deshabilitada en la cuenta de administrador, está deshabilitada en las cuentas de miembro. Este comportamiento se aplica a las cuentas de miembros nuevas y existentes.

Si deshabilita los resultados de control consolidados en su cuenta, Security Hub genera un resultado separado por control de seguridad para cada estándar habilitado que incluya un control. Por ejemplo, si cuatro estándares habilitados comparten un control con la misma AWS Config regla subyacente, 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 resultados de control consolidados, Security Hub crea resultados nuevos independientes de los estándares y archiva los resultados originales basados en estándares. Algunos campos y valores de resultado de controles cambiarán y pueden afectar a los flujos de trabajo existentes. Para obtener más 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. La [respuesta de seguridad automatizada de la AWS versión 2.0.0](#) respalda los hallazgos 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

Después de habilitar los resultados de control consolidados, Security Hub puede tardar hasta 24 horas en generar nuevos resultados consolidados y archivar los resultados originales basados en estándares. Del mismo modo, después de deshabilitar los resultados de control consolidados, Security Hub puede tardar hasta 24 horas en generar nuevos resultados basados en estándares y archivar los resultados consolidados. Durante ese tiempo, es posible que vea en su cuenta una combinación de resultados independientes de los estándares y resultados basados en estándares.

Security Hub console

Para habilitar o deshabilitar los resultados de control consolidados (consola)

1. Abra la AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>
2. En el panel de navegación, seleccione Configuración.
3. Elija la pestaña General.
4. En Controles, active o desactive los Resultados de control consolidados.
5. Seleccione Guardar.

Security Hub API, AWS CLI

Para activar o desactivar las conclusiones de control consolidadas (API, AWS CLI)

1. Utilice la operación [UpdateSecurityHubConfiguration](#). Si está utilizando el AWS CLI, ejecute el [update-security-hub-configuration](#) comando.
2. Establezca `control-finding-generator` en `SECURITY_CONTROL` para habilitar los resultados de control consolidados. Establezca `control-finding-generator` en `STANDARD_CONTROL` para deshabilitar los resultados de control consolidados.

Por ejemplo, el siguiente AWS CLI comando habilita los hallazgos de control consolidados. 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 --region us-east-1 update-security-hub-configuration --  
control-finding-generator SECURITY_CONTROL
```

El siguiente AWS CLI comando desactiva las conclusiones de control consolidadas. 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 --region us-east-1 update-security-hub-configuration --  
control-finding-generator STANDARD_CONTROL
```

Generar nuevos hallazgos en lugar de actualizar los hallazgos existentes

Security Hub ejecuta los controles de seguridad de forma [programada](#). 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 genera un nuevo hallazgo que contiene el resultado más reciente.

Si una comprobación posterior con respecto a una regla determinada genera un resultado idéntico al resultado actual, Security Hub actualiza el resultado existente. No se genera un nuevo hallazgo.

Security Hub archiva automáticamente los resultados de los controles si el recurso asociado se elimina, el recurso no existe o el control está deshabilitado. Es posible que un recurso ya no exista porque el servicio asociado no se utiliza actualmente. Los resultados se archivan automáticamente en función de uno de los siguientes criterios:

- El resultado no se actualiza hasta transcurridos entre 3 y 5 días (ten en cuenta que es lo mejor y no está garantizado).
- Se devolvió AWS Config la evaluación asociada NOT_APPLICABLE.

Controle, encuentre, automatice y suprima.

Puede usar las reglas de automatización de Security Hub para actualizar o suprimir hallazgos de control específicos. Si suprimes un hallazgo, seguirá estando accesible en tu cuenta, pero eso indica que crees que no es necesario tomar ninguna medida para solucionarlo. Al suprimir los hallazgos irrelevantes, puedes reducir el ruido que generan las búsquedas. 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 automáticamente los hallazgos, consulte [Descripción de las reglas de automatización en Security Hub](#).

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 no realiza controles de seguridad en él y no se te cobra nada.

Detalles de cumplimiento de las conclusiones sobre el control

En el caso de las conclusiones generadas por las comprobaciones de seguridad de los controles, el [Compliance](#) campo del formato de comprobación de AWS seguridad (ASFF) contiene detalles relacionados con las comprobaciones de control. El campo Compliance incluye la siguiente información.

AssociatedStandards

Los estándares habilitados en los que está habilitado un control.

RelatedRequirements

La lista de requisitos relacionados con el control en todos los estándares habilitados. Los requisitos provienen del marco de seguridad de terceros para el control, como el estándar de seguridad de datos del sector de las tarjetas de pago (PCIDSS).

SecurityControlId

El identificador de un control que cumple con los estándares de seguridad que admite Security Hub.

Status

El resultado de la última comprobación realizada por Security Hub para un control determinado. Los resultados de las comprobaciones anteriores se conservan en estado archivado durante 90 días.

StatusReasons

Contiene una lista de motivos para el valor `Compliance.Status`. Para cada motivo, `StatusReasons` incluye el código de motivo y una descripción.

En la siguiente tabla se enumeran los códigos de motivo de estado y las descripciones disponibles. Los pasos de corrección dependen del control que haya generado un resultado con el código de

motivo. Elija uno de los controles de [Referencia de controles de Security Hub](#) para ver los pasos de corrección de ese control.

Código de motivo	Compliance Status	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 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

Código de motivo	Compliance.Status	Descripción
		eliminaron los recursos especificados o se eliminaron los resultados de la evaluación.
CONFIG_RECORDER_CUSTOM_ROLE	FAILED(para Config.1)	La AWS Config grabadora usa un IAM rol 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 de Security Hub habilitados. Active la grabación de los siguientes recursos: <i>Resources that aren't being recorded.</i>

Código de motivo	Compliance Status	Descripción
CONFIG_RETURNS_NOT_APPLICABLE	NOT_AVAILABLE	<p>El estado de cumplimiento se NOT_AVAILABLE debe a que AWS Config devolvió el estado de No aplicable.</p> <p>AWS Config no indica el motivo del estado. Estas son algunas de las posibles razones del estado de No aplicable:</p> <ul style="list-style-type: none">• 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	Descripción
CONFIG_RULE_EVALUATION_ERROR	NOT_AVAILABLE AWS Config el estado es ConfigError	<p>Este código de motivo se utiliza para varios tipos diferentes de errores de evaluación.</p> <p>La descripción proporciona la información específica del motivo.</p> <p>El tipo de error puede ser uno de los siguientes:</p> <ul style="list-style-type: none"> • 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	<p>La AWS Config regla está en proceso de creación.</p>

Código de motivo	Compliance Status	Descripción
INTERNAL_SERVICE_ERROR	NOT_AVAILABLE	Se ha producido un error desconocido.
LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE	FAILED	Security Hub no puede realizar una comprobación con un tiempo de ejecución de Lambda personalizado.
S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION	WARNING	<p>El resultado se encuentra en un estado de WARNING, porque el bucket de S3 asociado a esta regla se encuentra en una región o cuenta diferente.</p> <p>Esta regla no admite comprobaciones entre regiones ni entre cuentas.</p> <p>Se recomienda deshabilitar este control en esta región o cuenta. Ejecútelo solo en la región o cuenta donde se encuentra el recurso.</p>
SNS_SUBSCRIPTION_NOT_PRESENT	FAILED	Los filtros métricos de CloudWatch Logs no tienen una SNS suscripción a Amazon válida.

Código de motivo	Compliance Status	Descripción
SNS_TOPIC_CROSS_ACCOUNT	WARNING	<p>El resultado se encuentra en un estado de WARNING.</p> <p>El SNS tema asociado a esta regla pertenece a una cuenta diferente. La cuenta actual no puede obtener la información de la suscripción.</p> <p>La cuenta propietaria del SNS tema debe conceder a la cuenta actual el <code>sns:ListSubscriptionsByTopic</code> permiso para el SNS tema.</p>
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	<p>El hallazgo se encuentra en un WARNING estado porque el SNS tema asociado a esta regla se encuentra en una región o cuenta diferente.</p> <p>Esta regla no admite comprobaciones entre regiones ni entre cuentas.</p> <p>Se recomienda deshabilitar este control en esta región o cuenta. Ejecútelos solo en la región o cuenta donde se encuentra el recurso.</p>
SNS_TOPIC_INVALID	FAILED	El SNS tema asociado a esta regla no es válido.
THROTTLING_ERROR	NOT_AVAILABLE	La API operación correspondiente ha superado la tasa permitida.

ProductFields detalles de los resultados del control

Cuando Security Hub ejecuta comprobaciones de seguridad y genera resultados de control, el [ProductFields](#) atributo in ASFF incluye los siguientes campos:

ArchivalReasons:0/Description

Describe por qué Security Hub ha archivado los resultados existentes.

Por ejemplo, Security Hub archiva los resultados existentes al deshabilitar un control o estándar y al activar o desactivar los [resultados del control consolidado](#).

ArchivalReasons:0/ReasonCode

Explica el motivo por el que Security Hub ha archivado los resultados existentes.

Por ejemplo, Security Hub archiva los resultados existentes al deshabilitar un control o estándar y al activar o desactivar los [resultados del control consolidado](#).

StandardsGuideArn o StandardsArn

El ARN del estándar asociado al control.

Para el estándar CIS AWS Foundations Benchmark, el campo esStandardsGuideArn.

Para PCI DSS los estándares AWS fundamentales de mejores prácticas de seguridad, el campo esStandardsArn.

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 CIS AWS Foundations Benchmark, el campo esStandardsGuideSubscriptionArn.

Para los estándares AWS fundamentales de mejores prácticas de seguridad PCI DSS y los estándares fundamentales, el campo esStandardsSubscriptionArn.

Estos campos se eliminan si habilita los [resultados de control consolidados](#).

RuleId o ControlId

El identificador del control.

Para el estándar CIS AWS Foundations Benchmark, 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`

URLA 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 resultados basados en el control, el nombre del producto es Security Hub.

`aws/securityhub/CompanyName`

Para los hallazgos 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](#).

Nivel de gravedad de los hallazgos de control

La gravedad asignada a un control 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 se 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.
- IAM existe la clave de usuario raíz.

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 capturar la información sobre la criticidad de los recursos, utilice el `Criticality` campo 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	Compromiso o muy poco probable
Muy fácil de explotar	Critico	Critico	Alta	Medio
Algo fácil de explotar	Critico	Alta	Medio	Medio
Algo difícil de explotar	Alta	Medio	Medio	Baja
Muy difícil de explotar	Medio	Medio	Baja	Baja

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 VPC seguridad predeterminado está abierto al tráfico entrante y saliente, se considera que es de gravedad alta. Es bastante fácil que un actor de amenazas comprometa una VPC con 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 recomienda tratar un resultado 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 recomienda que investigue el recurso implicado tan pronto como sea 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 control y el estado de conformidad en Security Hub

El `Compliance.Status` campo del formato de comprobación de AWS seguridad describe el resultado de una comprobación de control. Security Hub utiliza el estado de conformidad de los resultados de control para determinar un estado de control general. El estado de control se muestra en la página de detalles de un control de la consola de Security Hub.

Evaluación del estado de conformidad de los resultados de Security Hub

El estado de conformidad para cada resultado se asigna uno de los siguientes valores:

- **PASSED:** indica que el control superó el control de seguridad correspondiente a este resultado. Establece automáticamente el `Workflow.Status` de Security Hub como **RESOLVED**.

Si el `Compliance.Status` para un resultado cambia de `PASSED` a `FAILED`, `WARNING`, o `NOT_AVAILABLE`; y `Workflow.Status` era `NOTIFIED` o `RESOLVED`; entonces Security Hub establece el `Workflow.Status` automáticamente como `NEW`.

Si no dispone de los recursos correspondientes para un control, Security Hub produce un resultado `PASSED` a nivel de cuenta. Si tiene un recurso correspondiente para un control, pero luego lo elimina, Security Hub crea un resultado `NOT_AVAILABLE` y lo archiva inmediatamente. Al cabo de 18 horas, recibirá un resultado `PASSED` porque ya no dispone de los recursos correspondientes al control.

- `FAILED`: indica que el control no superó el control de seguridad correspondiente a este resultado.
- `WARNING`: indica que el control se completó, pero que Security Hub no puede determinar si el recurso tiene el estado `PASSED` o `FAILED`.
- `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 archiva automáticamente el hallazgo.

Obtención del estado de control a partir del estado de conformidad

Security Hub obtiene un estado de control general a partir del estado de conformidad de los resultados de control. Al determinar el estado de control, Security Hub ignora los resultados que tienen un `RecordState` como `ARCHIVED` y los resultados que tienen un `Workflow.Status` como `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 activado tiene este estado hasta que Security Hub comience a generar resultados para él. Un control también tiene este estado si todos los resultados son `SUPPRESSED` o si no están disponibles en la región actual.

- **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.

Para 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.

Por lo general, Security Hub genera el estado de control inicial 30 minutos después de la primera visita a la página Resumen o a la página Normas de seguridad de la consola 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 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

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) Region.

Calcular las puntuaciones de seguridad

La página Resumen y la página Controles de la consola de Security Hub muestran un resumen de la puntuación de seguridad de todos los estándares habilitados. En la página Estándares de seguridad, Security Hub también muestra una puntuación de seguridad del 0 al 100 por ciento para cada estándar habilitado.

Al activar Security Hub por primera vez, Security Hub calcula la puntuación de seguridad resumida y las puntuaciones de seguridad estándar en un plazo de 30 minutos después de su primera

visita a la página [Resumen](#) o a la página [Normas de seguridad](#) de la consola de Security Hub. Las puntuaciones solo se generan para los estándares que están activados al visitar esas páginas. Para ver una lista de los estándares que están habilitados actualmente, invoque la [GetEnabledStandards](#) API operación. 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.

Tras la primera generación de puntuaciones, Security Hub actualiza las puntuaciones de seguridad cada 24 horas. Security Hub muestra una marca de tiempo para indicar cuándo se actualizó por última vez una puntuación de seguridad.

Note

Las puntuaciones de seguridad por primera vez pueden tardar hasta 24 horas en generarse en las regiones de China y de AWS GovCloud (US) Region.

Si activa los [resultados de control consolidados](#), es posible que sus puntuaciones de seguridad tarden 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 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 calcula una puntuación de seguridad resumida para todos los estándares habilitados. Security Hub 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 ignora los resultados 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 control y el estado de conformidad en Security Hub](#).

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%
CIS AWS Foundations Benchmark v1.4.0	8	29	0	22%
CIS AWS Foundations Benchmark v1.2.0	6	35	0	15%
NIST Publicación especial 800-53, revisión 5	159	56	0	74%
PCIDSSv3.2.1	28	17	0	62%

Al calcular la puntuación de seguridad resumida, Security Hub 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 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 tengas una puntuación resumida diferente de la puntuación de seguridad estándar, incluso si solo has activado un estándar en tu 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 en las regiones enlazadas se han activado estándares adicionales o diferentes.

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 todos los estados de control 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.

Lista de categorías de control en Security Hub

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:

- Amazon VPC Flow Logs
- 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

Proteger

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?
- ¿El servicio utiliza la autenticación multifactorial (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/Usos de datos: ¿Utiliza servicios como Amazon Macie para rastrear la ubicación de sus datos confidenciales?

APIprotección

¿El servicio se utiliza AWS PrivateLink para proteger las API operaciones 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 las diez principales del 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, 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 EBS instantáneas de Amazon asociadas con resultados realmente 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?

Visualización de los detalles de un control

Al seleccionar un control de AWS Security Hub en la página Controles o en la página de detalles estándar de la consola 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 de control. El estado de control resume el rendimiento de un control en función del estado de conformidad de los resultados del control. Por lo general, Security Hub genera el estado de control inicial 30 minutos después de la primera visita a la página Resumen o a la página Normas de seguridad de la consola 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 control y el estado de conformidad en 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 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) Region.

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 en las últimas 24 horas. Los resultados del control se generan cuando Security Hub ejecuta los controles de seguridad en relación con el control. La lista de resultados de control 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 “Visualización y administración de los resultados de control”](#).

Visualización de detalles de un control

Elija su método de acceso preferido y siga estos pasos para ver los detalles de un control. Los detalles se aplican a la cuenta corriente y a la región e incluyen lo siguiente:

- Título y descripción del control
- Enlace a las instrucciones de corrección en caso de que se detecte un error en el control
- Gravedad del control
- Estado de habilitación del control

- (En la consola) Una lista de los resultados recientes del control. Cuando utilice la API de Security Hub o AWS CLI, utilice [GetFindings](#) para recuperar los resultados de control.

Security Hub console

1. Abra la consola de AWS Security Hub en <https://console.aws.amazon.com/securityhub/>.
2. En el panel de navegación, elija Control.
3. Seleccione un control.

Security Hub API

1. Ejecute [ListSecurityControlDefinitions](#) y proporcione uno o más ARN estándar para obtener una lista de los identificadores de control para ese estándar. Para obtener los ARN estándar, ejecute [DescribeStandards](#). Si no proporciona un ARN estándar, esta API devuelve todos los identificadores de control de Security Hub. Esta API devuelve los identificadores de control de seguridad independientes de los estándares, no los identificadores de control basados en estándares que existían antes de las versiones de estas características.

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 en las Región de AWS y Cuenta de AWS actuales.

Ejemplo de solicitud:

```
{
  "SecurityControlIds": ["Config.1", "IAM.1"]
}
```

AWS CLI

1. Ejecute el comando [list-security-control-definitions](#) y proporcione uno o más ARN estándar para obtener una lista de los identificadores de control. Para obtener los ARN estándar, ejecute el comando `describe-standards`. Si no proporciona un ARN estándar, este comando devuelve todos los identificadores de control de Security Hub. Este comando devuelve los identificadores de control de seguridad independientes de los estándares, no los identificadores de control basados en estándares que existían antes de las versiones de estas características.

```
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

En la página Controles de la consola de AWS Security Hub, verá una lista de todos los controles compatibles. También puede filtrar y ordenar la lista para centrarse en un subconjunto específico de controles.

Las opciones Filtrar por situadas junto a la lista de controles le permiten centrarse rápidamente en estos subconjuntos específicos:

- Todos los controles habilitados (controles que están habilitados en al menos un estándar habilitado)
- Todos los controles deshabilitados (controles que están deshabilitados en todos los estándares).
- Para los controles habilitados, aquellos con un estado de control específico (con fallos, aprobado, desconocido o sin datos). Sin datos son los controles sin resultados. Para obtener más información sobre el estado de control, consulte [Evaluación del estado de control y el estado de conformidad en Security Hub](#).

Además de las opciones Filtrar por, puede filtrar las listas de controles si introduce los filtros en el cuadro de búsqueda de Controles del filtro. Por ejemplo, puede filtrar por ID de control o gravedad.

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 Title o Description. Estos últimos campos podrían cambiar ocasionalmente, mientras que el ID de control y el ARN son identificadores estáticos.

Si inició sesión en una cuenta de administrador de Security Hub, los controles Habilitados incluyen los que están habilitados en al menos una cuenta de miembro. Si ha establecido una región de agregación, los controles Habilitados incluyen aquellos que están habilitados en al menos una región vinculada.

De forma predeterminada, los controles con el estado Con fallos aparecen primero, ordenados por gravedad decreciente. Puede cambiar el orden predeterminado si selecciona una opción diferente en los encabezados de las columnas.

Al seleccionar la opción situada junto al control, aparece un panel lateral 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 desactivándolo en todos los estándares. Para obtener instrucciones sobre cómo habilitar y deshabilitar controles en todos los estándares, consulte [Habilitación de controles en Security Hub](#). En el caso de las cuentas de administrador, la información presentada en el panel lateral refleja todas las cuentas de los miembros.

En la API de Security Hub, use la operación [ListSecurityControlDefinitions](#) para obtener una lista de los identificadores de control. Una vez que tenga los identificadores de control pertinentes, utilice la operación [BatchGetSecurityControls](#) para obtener datos sobre ese subconjunto de controles en la Cuenta de AWS y la Región de AWS actuales.

Descripción de los parámetros de control en Security Hub

Algunos controles AWS Security Hub 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. Sin embargo, para un subconjunto de estos controles,

puede modificar los valores de los parámetros. Al modificar el valor de un parámetro de un control, Security Hub comienza a evaluar el control con el valor que especifique. Si el recurso subyacente al control cumple con el valor personalizado, Security Hub genera un resultado PASSED. Si el recurso no cumple el valor personalizado, Security Hub genera un resultado FAILED.

Al personalizar los parámetros de control, puede refinar las prácticas recomendadas de seguridad que recomienda y supervisa Security Hub 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 IAM los usuarios deben tener configuraciones sólidas

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 VPC Lambda 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 genera nuevos resultados de control en función del nuevo valor. Durante las actualizaciones periódicas de los resultados del control, Security Hub también utiliza el nuevo valor del parámetro. Si cambia los valores de los parámetros de un control, pero no ha habilitado ningún estándar que lo incluya, Security Hub no

ejecutará ningún control de seguridad con los nuevos valores. Debe habilitar al menos un estándar pertinente para que Security Hub 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 para los controles 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 proporciona el rango aceptable.

Security Hub elige los valores de los parámetros predeterminados y puede actualizarlos ocasionalmente. 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 predeterminado de Security Hub, incluso si el valor personalizado del parámetro coincide con el valor predeterminado actual que define Security Hub. Este es un ejemplo del control [ACM.1]: los certificados importados y ACM emitidos deben renovarse después de un período 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 cambia el valor predeterminado a 14, el parámetro de este ejemplo no hará un seguimiento de ese cambio. Retendrá un valor de 30.

Si quiere hacer un seguimiento de las actualizaciones del valor predeterminado de Security Hub para un parámetro, establezca el campo `ValueType` en `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 [Controles de la consola de Security Hub](#) o la [Referencia de controles de Security Hub](#). Para recuperar esta lista mediante programación, puede utilizar el [ListSecurityControlDefinitions](#) operación. 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 AWS Security Hub administrador delegado 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 console

Para revisar los valores actuales de los parámetros de control (consola)

1. Abra la AWS Security Hub consola 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 API

Para revisar los valores actuales de los parámetros de control (API)

invoque el [BatchGetSecurityControls](#) API, y proporcione uno o más controles de seguridad IDs o 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 de `APIGateway.1`, `CloudWatch.15`, y `IAM.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 console

Para revisar los valores actuales de los parámetros de control en una política de configuración (consola)

1. Abra la AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>.

Inicie sesión con las credenciales de la cuenta de administrador delegado de Security Hub 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 API

Para revisar los valores actuales de los parámetros de control en una política de configuración (API)

1. Invoque el [GetConfigurationPolicy](#) API desde la cuenta de administrador delegado en la región de origen.
2. Proporcione el identificador ARN o ID de la política de configuración cuyos detalles desee 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 de Security Hub, elija Resultados del panel de navegación. Para revisar los resultados mediante programación, utilice la [GetFindings](#) funcionamiento del Security Hub API.

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 centralizada](#) en AWS Security Hub. La configuración central es una función que el administrador delegado del Security Hub puede utilizar para configurar las capacidades del Security Hub en todas Regiones de AWS las cuentas y unidades 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 en vigor en su región de

origen y en todas las regiones vinculadas. OUs 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 Security Hub de una organización que utiliza una configuración centralizada, elija el método que prefiera y siga las instrucciones para personalizar los parámetros de control en varias cuentas y regiones.

Security Hub console

Para personalizar los valores de un parámetro de control en varias cuentas y regiones (consola)

1. Abra la AWS Security Hub consola 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 o a las OUs que quieres aplicar la política.
6. Elija Next (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 Next (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 API

Para personalizar los valores de los parámetros de control en varias cuentas y regiones (API)

Para crear una política de configuración nueva con valores de parámetros de control personalizados

1. Invoque el [CreateConfigurationPolicy](#) API desde la cuenta de administrador delegado en 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, utilice la [GetSecurityControlDefinition](#) API.

Para personalizar los valores de un parámetro de control en una política de configuración existente

1. Invoque el [UpdateConfigurationPolicy](#) API desde la cuenta de administrador delegado en la región de origen.
2. Para el `Identifier` campo, proporciona el nombre del recurso de Amazon (ARN) o el ID de la política de configuración que deseas 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, invoca la [GetSecurityControlDefinition](#) API.

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 console

Para personalizar los valores de un parámetro de control en una cuenta y región (consola)

1. Abra la AWS Security Hub consola 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 Guardar.

Security Hub API

Para personalizar los valores de los parámetros de control en una cuenta y región (API)

1. Invoque el [UpdateSecurityControl](#) API.
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 compatibles para un control, invoque la [GetSecurityControlDefinition](#) API.
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 AWS Security Hub defina. En algunas ocasiones, Security Hub actualiza el valor predeterminado de un parámetro para reflejar la evolución de las prácticas recomendadas 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 centralizada](#) en Security Hub. La configuración central es una función que el administrador delegado del Security Hub puede utilizar para configurar las capacidades del Security Hub en todas Regiones de AWS las cuentas y unidades organizativas (OUs).

Note

No todos los parámetros de control tienen un valor predeterminado de Security Hub. En esos casos, cuando `ValueType` se establece en `DEFAULT`, no hay un valor predeterminado específico que utilice Security Hub. Por el contrario, Security Hub ignora el parámetro en ausencia de un valor personalizado.

Reversión a los parámetros de control predeterminados en varias cuentas y regiones

Si utiliza la configuración central, puede revertir los parámetros de control de varias cuentas administradas de forma centralizada y de la región OUs de origen y 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 console

Para revertir los valores predeterminados de los parámetros de control en varias cuentas y regiones (consola)

1. Abra la AWS Security Hub consola en <https://console.aws.amazon.com/securityhub/>

Inicie sesión con las credenciales de la cuenta de administrador delegado de Security Hub 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, verifica las cuentas o a las OUs que deseas aplicar la política.
8. Elija Next (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 API

Para volver a los valores de los parámetros de control predeterminados en varias cuentas y regiones () API

1. Invoque el [UpdateConfigurationPolicy](#) API desde la cuenta de administrador delegado en la región de origen.
2. Para el `Identifier` campo, proporciona el nombre del recurso de Amazon (ARN) o el ID de la política que deseas 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 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 campo `SecurityControlCustomParameters`, Security Hub 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 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 \  
--policy-id acm:1 \  
--control-id daysToExpiration \  
--value-type DEFAULT \  
--value 30 \  
--tags Key=Value \  
--output text \  
--profile admin \  
--role-arn arn:aws:iam::123456789012:role/SecurityHubAdmin \  
--region us-east-1 \  
--policy-id acm:1 \  
--control-id daysToExpiration \  
--value-type DEFAULT \  
--value 30 \  
--tags Key=Value \  
--output text \  
--profile admin \  
--role-arn arn:aws:iam::123456789012:role/SecurityHubAdmin
```

```
--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 Security Hub, se restablecen los parámetros de control personalizados. Si vuelve a habilitar Security Hub en el futuro, todos los controles utilizarán los valores predeterminados de los parámetros para comenzar.

Security Hub console

Para revertir los valores predeterminados de los parámetros de control en una cuenta o región (consola)

1. Abra la AWS Security Hub consola 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 utiliza el valor predeterminado de Security Hub y hace un seguimiento de las actualizaciones futuras hasta el valor predeterminado.
4. Repita el paso anterior para cada valor de parámetro que quiere revertir.

Security Hub API

Para volver a los valores de los parámetros de control predeterminados en una cuenta y una región () API

1. Invoque el [UpdateSecurityControl](#) API.
2. Para `SecurityControlId`, proporcione el ARN o ID del control cuyos parámetros desee 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 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 `daysToExpiration` de 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 completa correctamente, Security Hub retiene el valor actual del parámetro.

Para comprobar que se completó correctamente la actualización de un parámetro, puede revisar los detalles del control en la consola 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.

De forma programática, si su solicitud de actualización de un parámetro es válida, el valor del `UpdateStatus` campo es `UPDATING` una respuesta a [BatchGetSecurityControls](#) operación. 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 utiliza los valores de los parámetros de control actualizados al ejecutar los controles 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, Security Hub lo volverá a intentar automáticamente si lo ha AWS Config activado. Para obtener más información, consulte [Consideraciones antes de habilitar y configurar AWS Config](#).

Visualización y administración de los resultados de control

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 utilizar el AWS Security Hub API para recuperar una lista de los resultados y los detalles de los resultados.

Para obtener más información, consulte [Instrucciones para revisar los detalles y el historial de los 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 “Configurar el estado del flujo de trabajo”](#).

También puedes enviar los resultados 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](#)
- [Ejemplos de resultados de control en Security Hub](#)

Filtrado y clasificación de resultados de control

Si seleccionas un control en la página de controles de la AWS Security Hub consola o en la página de detalles de un estándar, accederás 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 utilizar la casilla Añadir filtro para filtrar la lista de verificación por otros campos, como el Cuenta de AWS identificador o el identificador del recurso.

De forma predeterminada, las conclusiones con un estado de conformidad de PASSED aparecen primero. 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 [Filtrar los resultados en Security Hub](#).

Ejemplos de resultados de control en Security Hub

El formato de los resultados de los controles varía en función de si se han activado los resultados de los controles consolidados. Al activar esta característica, Security Hub genera un único resultado para una comprobación de control, incluso cuando el control se aplica a varios estándares habilitados. Para obtener más información, consulte [Resultados de control consolidados](#).

En la siguiente sección se muestran ejemplos de resultados de control en formato AWS Security Finding Format (ASFF). Estos incluyen los resultados de cada estándar de Security Hub cuando los resultados de control consolidados están desactivados en su cuenta y un ejemplo de los resultados de control de todos los estándares cuando están activados.

Note

Los resultados harán referencia a diferentes campos y valores de las regiones de AWS GovCloud (US) y la región de China. Para obtener más información, consulte [Impacto de la consolidación en los campos y valores ASFF](#).

Los resultados de control consolidados están desactivados

- [Ejemplo de búsqueda del estándar AWS Foundational Security Best Practices \(FSBP\)](#)
- [Ejemplo de hallazgo para Center for Internet Security \(CIS\) AWS Foundations Benchmark v1.2.0](#)
- [Ejemplo de búsqueda para Center for Internet Security \(CIS\) AWS Foundations Benchmark v1.4.0](#)
- [Ejemplo de búsqueda para Center for Internet Security \(CIS\) AWS Foundations Benchmark v3.0.0](#)
- [Ejemplo de hallazgo para el Instituto Nacional de Estándares y Tecnología \(NIST\) SP 800-53 Rev. 5](#)
- [Ejemplo de búsqueda para el estándar de seguridad de datos de la industria de tarjetas de pago \(\) PCI DSS](#)
- [Ejemplo de búsqueda para AWS Resource Tagging Standard](#)
- [Ejemplo de hallazgo para Service-Managed Standard: AWS Control Tower](#)

Los resultados de control consolidados están activados

- [Ejemplo de resultado en todos los estándares](#)

Ejemplo de hallazgo para FSBP

```
{
  "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",
  "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 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/ProductName": "Security Hub",
    "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/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

```

{
  "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",
  "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 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",
  "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

```

{
  "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",
  "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 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",
    "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

```

{
  "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",
  "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 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",
    "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 el NIST SP 800-53 Rev. 5

```
{
  "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",
  "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 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",
    "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 para PCI DSS

```

{
  "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",
  "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 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",
      "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 AWS Resource Tagging Standard

```

{
  "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",
  "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 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",
    "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 Service-Managed Standard: AWS Control Tower

Note

Este estándar solo está disponible para usted si es un AWS Control Tower usuario que lo creó en. AWS Control Tower Para obtener más información, consulte [Estándar de gestión de servicios: AWS Control Tower](#).

```
{
  "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",
  "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 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",
  "aws/securityhub/CompanyName": "AWS",
  "Resources:0/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 resultado en todos los estándares (cuando la característica de resultado de control consolidada está activada)

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "security-control/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-10-06T02:18:23.076Z",
  "LastObservedAt": "2022-10-28T16:10:06.956Z",
  "CreatedAt": "2022-10-06T02:18:23.076Z",
  "UpdatedAt": "2022-10-28T16:10:00.093Z",
  "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 directions on how to correct this issue, consult the AWS Security
Hub controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
  "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
  "aws/securityhub/ProductName": "Security Hub",
  "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:security-control/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",
  "RelatedRequirements": [
    "PCI DSS v3.2.1/3.4",
    "CIS AWS Foundations Benchmark v1.2.0/2.7",
    "CIS AWS Foundations Benchmark v1.4.0/3.7"
  ],
  "SecurityControlId": "CloudTrail.2",
  "AssociatedStandards": [
    { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
    { "StandardsId": "standards/pci-dss/v/3.2.1"},
    { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
    { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
    { "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"
    ]
  }
}
```

Comprensión de las integraciones en Security Hub

AWS Security Hub puede asimilar los hallazgos de seguridad de varias soluciones Servicios de AWS de AWS Partner Network seguridad de terceros compatibles. Estas integraciones pueden ayudarlo a obtener una visión integral de la seguridad y el cumplimiento en todo su AWS entorno.

Security Hub recoge los resultados de las soluciones integradas y los convierte en el AWS Security Finding Format (ASFF).

Important

De las integraciones de productos compatibles AWS y de terceros, Security Hub recibe y consolida solo los hallazgos que se generan después de habilitar Security Hub en su. Cuentas de AWS

Este servicio no recibe ni consolida los resultados de seguridad que se generaron antes de que habilitara Security Hub de forma retroactiva.

La página de integraciones de la consola Security Hub proporciona acceso a las integraciones de productos disponibles AWS y de terceros. El Security Hub API también cuenta con operaciones para gestionar las integraciones.

Es posible que una integración no esté disponible en todas Regiones de AWS. Si no se admite una integración en la región en la que inició sesión en este momento en la consola de Security Hub, esta no aparecerá en la página de 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 que son compatibles en China \(Pekín\) y China \(Ningxia\)”](#) y [the section called “Integraciones compatibles en AWS GovCloud \(Este de EE. UU.\) y AWS GovCloud \(Oeste de EE. UU.\)”](#).

Además de las Servicio de AWS integraciones integradas de terceros, también puede integrar productos de seguridad personalizados con Security Hub. Para obtener más información, consulte [Integración de Security Hub a productos personalizados](#).

Visualización de una lista de las integraciones de Security Hub

Elige el método que prefieras y sigue los pasos para ver una lista de integraciones en AWS Security Hub o los detalles sobre una integración específica.

Security Hub console

Para ver los detalles y opciones de integración (consola)

1. Abra la consola AWS de Security Hub en <https://console.aws.amazon.com/securityhub/>.
2. En el panel de navegación de Security Hub, elija Integraciones.

En la página Integraciones, las integraciones con otros Servicios de AWS se enumeran primero, seguidas de 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 API

Para ver las opciones y los detalles de la integración (API)

Para obtener una lista de integraciones, usa la [DescribeProducts](#) operación. Si está utilizando el AWS CLI, ejecute el [describe-products](#) comando

Para recuperar los detalles de la integración de un producto específico, proporciona el nombre del recurso de Amazon (ARN) de la integración en el `ProductArn` campo.

Por ejemplo, el siguiente AWS CLI comando recupera detalles sobre la integración de Security Hub con 3CORESec. 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 describe-products --product-arn "arn:aws:securityhub:us-east-1::product/3coresec/3coresec"
```

Habilitación del flujo de resultados desde una integración

En la página Integraciones de la consola de AWS Security Hub, 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 de forma automática un permiso de nivel de recursos que permite a Security Hub recibir resultados del servicio.

En el caso de las integraciones de productos de terceros, es posible que tengas 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 necesita Security Hub para recibir los resultados 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 console

Para deshabilitar y habilitar el flujo de resultados desde una integración (consola)

1. Abra la consola AWS de Security Hub en <https://console.aws.amazon.com/securityhub/>.
2. En el panel de navegación de Security Hub, elija Integraciones.
3. Para las integraciones que envíen resultados, la información en Estado indica si Security Hub está aceptando resultados de esa integración en este momento.
4. Seleccione Aceptar los resultados.

Security Hub API

Utilizar [EnableImportFindingsForProduct](#) operación. Si está utilizando el AWS CLI, ejecute el [enable-import-findings-for-product](#) comando. Para permitir que Security Hub reciba los resultados de una integración, necesita el productoARN. 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 a Security Hub recibir los resultados 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"
```

Deshabilitación del flujo de resultados desde una integración

Elige el método que prefieras y sigue los pasos para deshabilitar el flujo de hallazgos de una integración de AWS Security Hub.

Security Hub console

Para deshabilitar el flujo de resultados desde una integración (consola)

1. Abra la consola AWS de Security Hub en <https://console.aws.amazon.com/securityhub/>.
2. En el panel de navegación de Security Hub, elija Integraciones.
3. Para las integraciones que envíen resultados, la información en Estado indica si Security Hub está aceptando resultados de esa integración en este momento.

4. Seleccione Dejar de aceptar resultados.

Security Hub API

Utilizar [DisableImportFindingsForProduct](#) operación. Si está utilizando el AWS CLI, ejecute el [disable-import-findings-for-product comando](#) Para deshabilitar el flujo de resultados de una integración, necesita la suscripción a ARN la integración habilitada. Para obtener la suscripción ARN, utilice la [ListEnabledProductsForImport](#) operación. Si está utilizando el AWS CLI, ejecute el [list-enabled-products-for-import](#).

Por ejemplo, el siguiente AWS CLI comando desactiva el flujo de hallazgos a Security Hub desde 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 disable-import-findings-for-product --product-subscription-arn  
"arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/  
crowdstrike-falcon"
```

Visualizar resultados desde una integración

Cuando empiece a aceptar las conclusiones de una integración de AWS Security Hub, la página Integraciones de la consola de Security Hub mostrará el estado de la integración como Aceptando las conclusiones. Para ver una lista de los resultados de la integración, seleccione Ver los resultados.

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 entre 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

AWS Security Hub 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 que son compatibles en China \(Pekín\) y China \(Ningxia\)”](#) y [the section called “Integraciones compatibles en AWS GovCloud \(Este de EE. UU.\) y AWS GovCloud \(Oeste de EE. UU.\)”](#).

A menos que se indique a continuación, Servicio de AWS las integraciones que envían los resultados a Security Hub se activan automáticamente después de activar Security Hub y el otro servicio. Las integraciones que reciben resultados 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

Esta es una descripción general de AWS los servicios que envían las conclusiones a Security Hub o reciben las conclusiones de Security Hub.

AWS Servicio integrado	Dirección
AWS Config	Envía resultados
AWS Firewall Manager	Envía resultados
Amazon GuardDuty	Envía resultados

AWS Servicio integrado	Dirección	
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	
AWS Chatbot	Recibe resultados	
Amazon Detective	Recibe resultados	
Amazon Security Lake	Recibe resultados	
AWS Systems Manager Explorer y OpsCenter	Recibe y actualiza resultados	
AWS Trusted Advisor	Recibe resultados	

AWS servicios que envían los resultados a Security Hub

Los siguientes AWS servicios se integran con Security Hub mediante el envío de los resultados a Security Hub. Security Hub convierte los resultados al [Formato de resultados de seguridad de AWS](#).

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 usar la integración con AWS Config, puede ver los resultados de las evaluaciones de reglas AWS Config administradas y personalizadas como hallazgos en Security Hub. Estos resultados se pueden ver junto con otros resultados de Security Hub, lo que proporciona una visión general completa de su estrategia de seguridad.

AWS Config usa Amazon EventBridge para enviar evaluaciones de AWS Config reglas a Security Hub. Security Hub transforma las evaluaciones de reglas en resultados con [Formato de resultados de seguridad de AWS](#). Luego, Security Hub 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

Todos los resultados de Security Hub utilizan el JSON formato estándar de ASFF. 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 a través de EventBridge. Security Hub transforma las evaluaciones de las reglas en conclusiones que siguen ASFF y enriquece las conclusiones haciendo todo lo posible.

Tipos de hallazgos que se AWS Config envían a Security Hub

Una vez activada la integración, AWS Config envía las evaluaciones de todas las reglas AWS Config administradas y las reglas personalizadas a Security Hub. Solo se envían las evaluaciones que se realizaron después de activar Security Hub. Por ejemplo, supongamos que la evaluación de una AWS Config regla revela cinco recursos fallidos. Si activo Security Hub después de eso y la regla revela un sexto recurso fallido, AWS Config envía solo la evaluación del sexto recurso a Security Hub.

Se excluyen las evaluaciones de [AWS Config las reglas vinculadas a servicios](#), como las que se utilizan para ejecutar comprobaciones en los controles de Security Hub.

Envío de AWS Config los resultados a Security Hub

Cuando se active la integración, Security Hub asignará automáticamente los permisos necesarios para recibir las conclusiones AWS Config. Security Hub utiliza permisos de service-to-service nivel que te proporcionan una forma segura de activar esta integración e importar los resultados AWS Config desde Amazon EventBridge.

Latencia para el envío de resultados

Cuando AWS Config crea un nuevo hallazgo, normalmente puedes verlo en Security Hub en cinco minutos.

Reintento cuando Security Hub no está disponible

AWS Config envía las conclusiones a Security Hub haciendo todo lo posible. EventBridge Cuando un evento no se envía correctamente a Security Hub, 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

Después AWS Config de enviar un hallazgo a Security Hub, este puede enviar actualizaciones del mismo hallazgo al Security Hub 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, se envían actualizaciones a Security Hub. Security Hub borra los resultados al cabo de 90 días desde la última actualización o 90 días después de que se crearan si no hay actualizaciones.

Security Hub no archiva las conclusiones que se envían AWS Config incluso si se elimina el recurso asociado.

Regiones en las que existen AWS Config hallazgos

AWS Config los hallazgos se producen a nivel regional. AWS Config envía las conclusiones al Security Hub de la misma región o regiones en las que se producen.

Visualización de AWS Config los resultados en Security Hub

Para ver sus AWS Config hallazgos, elija Hallazgos en el panel de navegación de Security Hub. Para filtrar los resultados y mostrar solo AWS Config los hallazgos, elija el nombre del producto en el menú desplegable de la barra de búsqueda. Introduzca Config y seleccione Aplicar.

Interpretación de la AWS Config búsqueda de nombres en Security Hub

Security Hub transforma las evaluaciones de 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 ASFF. La siguiente tabla mapea los campos de evaluación de AWS Config reglas con sus ASFF homólogos tal como aparecen en Security Hub.

Configuración de tipo de resultado de la evaluación de reglas	ASFF tipo de búsqueda	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"
	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: \${detail.ConfigRuleName} “
Se calculó el elemento de configuración ARN "" o Security Hub ARN	Resources[i].id	

Configuración de tipo de resultado de la evaluación de reglas	ASFF tipo de búsqueda	Valor codificado
detalle. 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"]
detalle. newEvaluationResult.complianceType	Compliance.Status	"FAILED«, " NOT _ AVAILABLE «, " PASSED o "WARNING»
	Workflow.Status	«RESOLVED" si se genera una AWS Config constatación con un Compliance.Status de "»PASSED, o si el Complianc e.Status cambia de "" a "».» FAILED PASSED De lo contrario, Workflow.Status será «.» NEW Puede cambiar este valor con la operación. BatchUpdateFindingsAPI

Interpretación de la etiqueta de gravedad

Todos los resultados de las evaluaciones de las AWS Config reglas tienen una etiqueta de MEDIUM gravedad predeterminada de ASFF. Puede actualizar la etiqueta de gravedad de un hallazgo con la [BatchUpdateFindings](#) API operación.

Hallazgo típico de AWS Config

Security Hub transforma las evaluaciones de AWS Config reglas en hallazgos que siguen las ASFF. El siguiente es un ejemplo de un hallazgo típico AWS Config de ASFF.

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, esta integración se activa automáticamente. AWS Config comienza inmediatamente a enviar los resultados a Security Hub.

Interrupción de la publicación de resultados en Security Hub

Para dejar de enviar los resultados a Security Hub, puedes usar la consola de Security Hub o el Security HubAPI.

Para obtener instrucciones sobre cómo detener el flujo de resultados, consulte [Habilitación del flujo de resultados desde una integración](#).

AWS Firewall Manager (Envía los resultados)

Firewall Manager envía los resultados a Security Hub cuando una política de firewall de aplicaciones web (WAF) para recursos o una regla de lista de control de acceso web (webACL) no cumple con las normas. Firewall Manager también envía los resultados cuando AWS Shield Advanced no protege los recursos o cuando se identifica un ataque.

Tras activar Security Hub, esta integración se activa automáticamente. Firewall Manager comienza a enviar inmediatamente resultados a Security Hub.

Para obtener más información sobre la integración, consulte la página Integraciones de la consola 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 a Security Hub. 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 a Security Hub 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 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.

Tras activar Security Hub, esta integración se activa automáticamente. GuardDuty comienza inmediatamente a enviar los resultados a Security Hub.

Para obtener más información sobre la GuardDuty integración, consulte [Integración con AWS Security Hub](#) en la Guía del GuardDuty 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 los resultados a Security Hub.

Para obtener más información sobre la integración, consulte las siguientes secciones.

Cómo AWS Health envía los resultados a Security Hub

En Security Hub, los problemas de seguridad se rastrean como resultados. Algunos hallazgos provienen de problemas detectados por otros AWS servicios o por socios externos. Security Hub también cuenta con un conjunto de reglas que utiliza para detectar problemas de seguridad y generar resultados.

Security Hub proporciona herramientas para administrar los resultados de todas estas fuentes. Puede ver y filtrar listas de resultados y ver los detalles de una búsqueda. Consulte [Revisión de los detalles de resultados y el historial de resultados en Security Hub](#). También puede realizar un seguimiento del estado de una investigación sobre un resultado. Consulte [Configuración del estado de flujo de trabajo de los resultados de Security Hub](#).

Todos los hallazgos de Security Hub utilizan un JSON formato 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 hallazgo.

AWS Health es uno de los AWS servicios que envía los resultados a Security Hub.

Tipos de hallazgos que se AWS Health envían a Security Hub

Una vez habilitada la integración, AWS Health envía los resultados que cumplen con una o más de las especificaciones enumeradas a Security Hub. Security Hub ingiere los resultados en [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 está el AWS Health servicio `risk` o `abuse`

Envío de AWS Health los resultados a Security Hub

Cuando decidas aceptar las conclusiones de AWS Health, Security Hub asignará automáticamente los permisos necesarios para recibir las conclusiones AWS Health. Security Hub utiliza permisos de `service-to-service` nivel que te proporcionan una forma fácil y segura de habilitar esta integración e importar los resultados AWS Health desde Amazon EventBridge en tu nombre. Si se selecciona Aceptar hallazgos, se otorga permiso a Security Hub para consumir los hallazgos de AWS Health.

Latencia para el envío de resultados

Cuando AWS Health crea un nuevo hallazgo, normalmente se envía a Security Hub en un plazo de cinco minutos.

Reintento cuando Security Hub no está disponible

AWS Health envía las conclusiones a Security Hub haciendo todo lo posible. EventBridge Cuando un evento no se envía correctamente a Security Hub, EventBridge vuelve a intentar enviar el evento durante 24 horas.

Actualización de los resultados existentes en Security Hub

Después AWS Health de enviar un hallazgo a Security Hub, este puede enviar actualizaciones al mismo hallazgo para reflejar observaciones adicionales de la actividad de búsqueda a Security Hub.

Regiones en las que existen resultados

Para eventos globales, AWS Health envía los resultados al Security Hub en us-east-1 (partición), cn-northwest-1 AWS (partición de China) y -1 (partición). gov-us-west GovCloud AWS Health envía los eventos específicos de la región al Security Hub de la misma región o regiones en las que se producen los eventos.

Visualización de AWS Health los resultados en Security Hub

Para ver sus AWS Health hallazgos en Security Hub, elija Hallazgos 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 de la AWS Health búsqueda de nombres en Security Hub

AWS Health envía los resultados a Security Hub mediante [AWS Formato de búsqueda de seguridad \(ASFF\)](#). AWS Health la búsqueda utiliza un patrón de eventos diferente al del ASFF formato Security Hub. En la siguiente tabla se detallan todos los campos de AWS Health búsqueda con sus ASFF homólogos tal y como aparecen en Security Hub.

Tipo de resultado de Estado	ASFFtipo de búsqueda	Valor codificado
cuenta	AwsAccountId	
detalle. startTime	CreatedAt	
detalle. eventDescription. latestDescription	Descripción	
detalle. eventTypeCode	GeneratorId	
detalle. eventArn (incluida la cuenta) más detalles. startTime	Id	

Tipo de resultado de Estado	ASFFtipo de búsqueda	Valor codificado
<region>«arn:aws:securityhub::» product/aws/health	ProductArn	
cuenta o resourceid	Resources[i].id	
	Resources[i].Type	“Otros”
	SchemaVersion	“10/08/2018”
	Severity.Label	Consultar “Interpretación de la etiqueta de gravedad” a continuación
detalle «AWS Health -». eventTypeCode	Título	
-	Tipos	[“Comprobaciones de configuración y software”]
event.time	UpdatedAt	
URLdel evento en la consola Health	SourceUrl	

Interpretación de la etiqueta de gravedad

La etiqueta de gravedad del ASFF hallazgo se determina mediante la siguiente lógica:

- Gravedad CRITICALsi:
 - 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 HIGHsi:

- 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 MEDIUMsi:

- 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 a Security Hub 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, esta integración se activa automáticamente. AWS Health comienza inmediatamente a enviar los resultados a Security Hub.

Interrupción de la publicación de resultados en Security Hub

Para dejar de enviar los resultados a Security Hub, puedes usar la consola de Security Hub o el Security HubAPI.

Para obtener instrucciones sobre cómo detener el flujo de resultados, consulte [Habilitación del flujo de resultados desde una integración](#).

AWS Identity and Access Management Access Analyzer (Envía los resultados)

Con IAM Access Analyzer, todos los resultados se envían a Security Hub.

IAM Access Analyzer utiliza un razonamiento basado en la lógica para analizar las políticas basadas en los recursos que se aplican a los recursos compatibles de su cuenta. IAM Access Analyzer genera un hallazgo cuando detecta una declaración de política que permite a un principal externo acceder a un recurso de su 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 organizaciones, el `AwsAccountId ASFF` campo refleja el ID de la cuenta del administrador. Bajo `ProductFields`, el campo `ResourceOwnerAccount` indica la cuenta en la que se descubrió el resultado. Si habilita los analizadores de cada cuenta individualmente, Security Hub genera varios resultados, uno que identifica el ID de la cuenta de administrador y otro que identifica el ID de la cuenta de recursos.

Para obtener más información, consulte [Integración con AWS Security Hub](#) en la Guía del IAM usuario.

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, esta integración se activa automáticamente. Amazon Inspector comienza a enviar a Security Hub inmediatamente todos los resultados que genera.

Para obtener más información sobre la integración, consulte [Integración con AWS Security Hub](#) en la Guía del usuario de Amazon Inspector.

Security Hub también puede recibir resultados desde Amazon Inspector Classic. Amazon Inspector Classic envía resultados de Security Hub que se generan a través de ejecuciones de evaluación para todos los paquetes de reglas compatibles.

Para obtener más información sobre la integración, consulte [Integración con AWS Security Hub](#) en la Guía del usuario de Amazon Inspector Classic.

Los resultados de Amazon Inspector y Amazon Inspector Classic utilizan el mismo productoARN. 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 Security Hub como Security Hub, visita la [página de integraciones de la consola de Security Hub](#) y selecciona Aceptar resultados para Auditar, Detectar o ambas opciones. AWS IoT Device Defender Audit and Detect comienza a enviar todos los resultados a Security Hub.

AWS IoT Device Defender La auditoría envía los resúmenes de las comprobaciones a Security Hub, que contienen información general sobre un tipo de comprobación de auditoría y una tarea de auditoría específicos. AWS IoT Device Defender Detect envía las conclusiones de infracciones

relacionadas con el aprendizaje automático (ML), las estadísticas y los comportamientos estáticos a Security Hub. Audit también envía actualizaciones de resultados a Security Hub.

Para obtener más información sobre esta integración, consulte [Integración con AWS Security Hub](#) en la Guía para AWS IoT desarrolladores.

Amazon Macie (Envía resultados)

Una conclusión de Macie puede indicar que existe una posible infracción de la política o que hay datos confidenciales, como información de identificación personal (PII), en los datos que su organización almacena en Amazon S3.

Después de activar Security Hub, Macie comienza a enviar automáticamente los resultados de las políticas a Security Hub. Puede configurar la integración para que también envíe resultados de datos confidenciales a Security Hub.

En Security Hub, el tipo de búsqueda de una política o de datos confidenciales se cambia a un valor compatible con ASFF. Por ejemplo, el tipo de resultado `Policy:IAMUser/S3BucketPublic` en Macie se muestra como `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic` en Security Hub.

Macie también envía resultados de muestra generados a Security Hub. 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 [Integración de Amazon Macie con AWS Security Hub](#) en la Guía del usuario de Amazon Macie.

AWS Systems Manager Administrador de parches (envía los resultados)

AWS Systems Manager Patch Manager envía los resultados a Security Hub 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, esta integración se activa automáticamente. Systems Manager Patch Manager comienza a enviar inmediatamente resultados a Security Hub.

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

Los siguientes AWS servicios están integrados con Security Hub y reciben los resultados de Security Hub. Cuando se indique lo contrario, el servicio integrado también puede actualizar resultados. En este caso, las actualizaciones de resultados que realice en el servicio integrado también se reflejarán en Security Hub.

AWS Audit Manager (Recibe los resultados)

AWS Audit Manager recibe las conclusiones de Security Hub. 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 admitidas por AWS Audit Manager](#) enumeran los controles para los que Security Hub envía resultados a Audit Manager.

AWS Chatbot (Recibe los resultados)

AWS Chatbot es un agente interactivo que te ayuda a supervisar tus AWS recursos e interactuar con ellos en tus canales de Slack y salas de chat de Amazon Chime.

AWS Chatbot recibe las conclusiones de Security Hub.

Para obtener más información sobre la AWS Chatbot integración con Security Hub, consulte la [descripción general de la integración con Security Hub](#) en la Guía AWS Chatbot del administrador.

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 con Detective te permite pasar de los GuardDuty hallazgos de Amazon en Security Hub a Detective. A continuación, puede utilizar las herramientas y visualizaciones de Detective para investigarlos. La integración no requiere ninguna configuración adicional en Security Hub o Detective.

Para los hallazgos recibidos de otros Servicios de AWS, el panel de detalles de los hallazgos de la consola de Security Hub incluye la 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 resultados 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 como fuente en la consola de Security Lake, Security Lake API o AWS CLI. Cuando complete estos pasos, Security Hub empezará a enviar todos los resultados a Security Lake.

Security Lake normaliza automáticamente los hallazgos de Security Hub y los 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 resultados de Security Hub.

Para obtener más información sobre esta integración, incluidas las instrucciones sobre cómo añadir Security Hub como fuente y crear suscriptores, consulte [Integración con AWS Security Hub](#) 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 de Security Hub y actualícelas en Security Hub.

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 ambos Trusted Advisor y Security Hub, la integración se actualiza automáticamente.

Security Hub envía los resultados de sus comprobaciones de mejores prácticas de seguridad AWS fundamentales a Trusted Advisor.

Para obtener más información sobre la integración de Security Hub con Trusted Advisor, consulte [Visualización de los controles de AWS Security Hub AWS Trusted Advisor en](#) la Guía del usuario de AWS Support.

Integraciones de productos de terceros con Security Hub

AWS Security Hub se integra con varios productos de socios de terceros. Una integración puede realizar una o más de las siguientes acciones:

- Enviar los resultados que genere a Security Hub
- Recibir resultados de Security Hub
- Actualizar resultados en Security Hub

Las integraciones que envían los resultados a Security Hub tienen un nombre de recurso de Amazon (ARN).

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 que son compatibles en](#)

[China \(Pekín\) y China \(Ningxia\)](#) y the section called “Integraciones compatibles en AWS GovCloud (Este de EE. UU.) y AWS GovCloud (Oeste de EE. UU.)”.

Si tiene una solución de seguridad y está interesado en convertirse en socio de Security Hub, envíe un correo electrónico a <securityhub-partners@amazon.com>. Para obtener más información, consulte la [Guía de integración de socios de AWS Security Hub](#).

Descripción general de integraciones de terceros con Security Hub

Este es un resumen sobre las integraciones de terceros que envían resultados a Security Hub o reciben resultados de Security Hub:

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/armor

Integración	Dirección	ARN (si corresponde)
		defense/armoranywhere
AttackIQ – AttackIQ	Envía resultados	arn:aws:securityhub: <REGION>::product/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

Integración	Dirección	ARN (si corresponde)
Claroty – xDome	Envía resultados	arn:aws:securityhub: <REGION>::product/claroty/xdome
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 resultados a Security Hub

Las siguientes integraciones de socios de terceros envían resultados a Security Hub. Security Hub convierte los resultados en [Formato de resultados de seguridad de AWS](#).

3CORESec – 3CORESec NTA

Tipo de integración: Enviar

ProductoARN: arn:aws:securityhub:<REGION>:product/3coresec/3coresec

3CORESec proporciona servicios de detección gestionados tanto para sistemas locales como para AWS sistemas. Su integración con Security Hub permite ver amenazas como malware, elevación de privilegios, movimiento lateral y segmentación inadecuada de la red.

[Enlace al producto](#)

[Documentación de socios](#)

Alert Logic – SIEMless Threat Management

Tipo de integración: Enviar

ProductoARN: `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 AWS WAF, y opciones de SOC analistas asignadas.

[Enlace al producto](#)[Documentación de socios](#)

Aqua Security – Aqua Cloud Native Security Platform

Tipo de integración: Enviar

ProductoARN: `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 canalización de CI/CD hasta los entornos de producción en tiempo de ejecución.

[Enlace al producto](#)[Documentación de socios](#)

Aqua Security – Kube-bench

Tipo de integración: Enviar

Producto: ARN `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-bench es una herramienta de código abierto que ejecuta el Kubernetes Benchmark del Center for Internet Security (CIS) en comparación con su entorno.

[Enlace al producto](#)[Documentación de socios](#)

Armor – Armor Anywhere

Tipo de integración: Enviar

Producto: ARN `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

ProductoARN: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platform emula un comportamiento adverso real alineado con el marco MITRE ATT &CK para ayudar a validar y mejorar su postura general de seguridad.

[Enlace al producto](#)

[Documentación de socios](#)

Barracuda Networks – Cloud Security Guardian

Tipo de integración: Enviar

Producto: ARN `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentry ayuda a las organizaciones a mantenerse seguras al crear aplicaciones y trasladar las cargas de trabajo a la nube pública.

[AWS Enlace a Marketplace](#)

[Enlace al producto](#)

BigID – BigID Enterprise

Tipo de integración: Enviar

ProductoARN: arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise

La BigID Enterprise Privacy Management Platform ayuda a las empresas a gestionar y proteger los datos confidenciales (PII) en todos sus sistemas.

[Enlace al producto](#)

[Documentación de socios](#)

Blue Hexagon – Blue Hexagon para AWS

Tipo de integración: Enviar

ProductoARN: 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

ProductoARN: 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

ProductoARN: `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

ProductoARN: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDome ayuda a las organizaciones a proteger sus sistemas ciberfísicos en todo el Internet ampliado de las cosas (XIoT) 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

Producto: ARN `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Security proporciona análisis antivirus y antimalware nativos de 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

ProductoARN: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assess es una IAST herramienta que ofrece detección de vulnerabilidades en tiempo real en aplicaciones web y microservicios. APIs Contrast Assess se integra con Security Hub 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

ProductoARN: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

La CrowdStrike Falcon Un sensor único y ligero unifica el antivirus de última generación, la detección y respuesta de los terminales y la búsqueda gestionada ininterrumpida en la nube.

[AWS Enlace a Marketplace](#)

[Documentación de socios](#)

CyberArk – Privileged Threat Analytics

Tipo de integración: Enviar

ProductoARN: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analytics recopilan, detectan, alertan y responden a las actividades y comportamientos de alto riesgo de las cuentas privilegiadas para contener los ataques en curso.

[Enlace al producto](#)

[Documentación de socios](#)

Data Theorem – Data Theorem

Tipo de integración: Enviar

Producto: ARN `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

ProductoARN: `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 ISO, y GDPR. La integración entre Drata y 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

ProductoARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASB le permite descubrir el uso de las aplicaciones en la nube, analizar los riesgos y aplicar los controles adecuados para las aplicaciones SaaS y personalizadas.

[Enlace al producto](#)

[Documentación de socios](#)

Forcepoint – Forcepoint Cloud Security Gateway

Tipo de integración: Enviar

ProductoARN: `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

ProductoARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLP aborda el riesgo centrado en las personas con visibilidad y control en todos los lugares donde trabajan sus empleados y dondequiera que residan sus datos.

[Enlace al producto](#)

[Documentación de socios](#)

Forcepoint – Forcepoint NGFW

Tipo de integración: Enviar

ProductoARN: `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

ProductoARN: `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 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

Producto: ARN `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centra proporciona visualización de flujos, microsegmentación y detección de brechas para cargas de trabajo en centros de datos y nubes modernos.

[Enlace al producto](#)

[Documentación de socios](#)

HackerOne – Vulnerability Intelligence

Tipo de integración: Enviar

Producto: ARN `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

La HackerOne la plataforma 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 HackerOne los hackers éticos han validado y proporcionado los pasos para reproducirlas.

[AWS enlace al mercado](#)

[Documentación de socios](#)

JFrog – Xray

Tipo de integración: Enviar

ProductoARN: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xray es una herramienta universal de análisis de la composición del software de seguridad de aplicaciones (SCA) que escanea continuamente los archivos binarios para comprobar el cumplimiento de las licencias y las vulnerabilidades de seguridad, de modo 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

ProductoARN: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks' El firewall SRX virtual de última generación ofrece un firewall virtual completo basado en la nube con seguridad avanzadaWAN, SD segura, redes sólidas y automatización integrada.

[AWS Enlace a Marketplace](#)

[Documentación de socios](#)

[Enlace al producto](#)

k9 Security – Access Analyzer

Tipo de integración: Enviar

ProductoARN: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Security le notifica cuando se producen cambios de acceso importantes en su AWS Identity and Access Management cuenta. With k9 Security, puede comprender el acceso que tienen los usuarios y las IAM funciones a sus datos críticos Servicios de AWS y a sus datos.

k9 Security está diseñado para una entrega continua, lo que le permite operar IAM con auditorías de acceso procesables y una automatización de políticas sencilla para AWS CDK Terraform y Terraform.

[Enlace al producto](#)

[Documentación de socios](#)

Lacework – Lacework

Tipo de integración: Enviar

Producto: ARN `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

ProductoARN: `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 (CSPM) y la plataforma de protección de la carga de trabajo en la nube (CWPP) para su AWS entorno.

[Enlace al producto](#)

[Documentación de socios](#)

NETSCOUT – NETSCOUT Cyber Investigator

Tipo de integración: Enviar

ProductoARN: `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

Producto: ARN `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Compute es una plataforma de ciberseguridad nativa de la nube que protege VMs los contenedores y las plataformas sin servidor.

[Enlace al producto](#)

[Documentación de socios](#)

Palo Alto Networks – Prisma Cloud Enterprise

Tipo de integración: Enviar

ProductoARN: `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

ProductoARN: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerion es una plataforma de seguridad en la nube con un enfoque único basado en las amenazas y el riesgo que ofrece medidas preventivas, detectivas y correctivas en todas sus cargas de trabajo. La integración entre 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

ProductoARN: `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

ProductoARN: `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

ProductoARN: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVM proporciona administración de vulnerabilidades para los entornos modernos, lo que le permite encontrar, priorizar y solucionar eficazmente las vulnerabilidades.

[Enlace al producto](#)

[Documentación de socios](#)

SecureCloudDB – SecureCloudDB

Tipo de integración: Enviar

ProductoARN: `arn:aws:securityhub:<REGION>::product/secureclouddb/secureclouddb`

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. 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

ProductoARN: `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 la IA en puntos finales, contenedores, cargas de trabajo en la nube y dispositivos de IoT.

[AWS Enlace a Marketplace](#)

[Enlace al producto](#)

Snyk

Tipo de integración: Enviar

ProductoARN: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snyk proporciona una plataforma de seguridad que analiza los componentes de la aplicación para detectar riesgos de seguridad en las cargas de trabajo en las que se estén ejecutando. AWS Estos riesgos se envían a Security Hub como 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

ProductoARN: `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 postura de seguridad y cumplimiento.

[Enlace al producto](#)[Documentación de socios](#)

Sophos – Server Protection

Tipo de integración: Enviar

Producto: ARN `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

ProductoARN: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRox ayuda a las empresas a proteger sus despliegues de contenedores y Kubernetes a escala mediante el cumplimiento de sus políticas de cumplimiento y seguridad durante 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

Producto: ARN `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logic es una plataforma segura de análisis de datos automatizados que permite a los equipos de operaciones de desarrollo y seguridad crear, ejecutar y proteger sus AWS aplicaciones.

[Enlace al producto](#)

[Documentación de socios](#)

Symantec – Cloud Workload Protection

Tipo de integración: Enviar

ProductoARN: `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

Producto: ARN `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

ProductoARN: `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 a Security Hub en tiempo real, lo que mejora la visibilidad de sus AWS recursos y Trend Micro Cloud One detalles del evento en Security Hub.

[AWS Enlace a Marketplace](#)

[Documentación de socios](#)

Vectra – Cognito Detect

Tipo de integración: Enviar

ProductoARN: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectra está transformando la ciberseguridad mediante la aplicación de una 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

ProductoARN: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wiz analiza continuamente las configuraciones, las vulnerabilidades, las redes, los IAM ajustes, los secretos y más de sus Cuentas de AWS usuarios y cargas de trabajo para descubrir problemas críticos que representan un riesgo real. Integre Wiz con Security Hub para visualizar y responder a los problemas que Wiz detecta desde la consola de Security Hub.

[AWS Enlace a Marketplace](#)

[Documentación de socios](#)

Integraciones de terceros que reciben resultados de Security Hub

Las siguientes integraciones de socios de terceros reciben resultados de Security Hub. Cuando se indique, los productos también pueden actualizar resultados. En este caso, las actualizaciones de resultados que realice en el producto del socio también se reflejarán en Security Hub.

Atlassian - Jira Service Management

Tipo de integración: Recibir y actualizar

El AWS Service Management Connector para Jira envía los resultados desde Security Hub a Jira. Jira los problemas se crean en función de los hallazgos. Cuando el Jira los problemas se actualizan y las conclusiones correspondientes se actualizan en Security Hub.

La integración solo es compatible con Jira Server y Jira Data Center.

Para obtener información general sobre la integración y su funcionamiento, vea el vídeo [AWS Security Hub: 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 para AWS Service Management Connector Jira envía los resultados desde Security Hub a Jira. Los resultados desencadenan la creación de problemas en . Jira Service Management Cloud. Cuando actualizas esos problemas en Jira Service Management Cloud, las conclusiones correspondientes también se actualizan en Security Hub.

[Enlace al producto](#)

[Documentación de socios](#)

Atlassian – Opsgenie

Tipo de integración: Recibir

Opsgenie es una solución moderna de gestión de incidentes para operar servicios siempre activos, que permite a los equipos de desarrollo y operaciones planificar las interrupciones del servicio y mantener el control durante los incidentes.

La integración con Security Hub garantiza que los incidentes críticos relacionados con la seguridad se dirigen a los equipos adecuados para su resolución inmediata.

[Enlace al producto](#)

[Documentación de socios](#)

Fortinet – FortiCNP

Tipo de integración: Recibir

FortiCNP es un producto de protección nativo de la nube que agrupa los hallazgos de seguridad en información útil y prioriza la información de seguridad en función de la puntuación de riesgo para reducir la fatiga de las alertas y acelerar la remediación.

[AWS Enlace a Marketplace](#)

[Documentación de socios](#)

IBM – QRadar

Tipo de integración: Recibir

IBM QRadar SIEM proporciona a los equipos de seguridad la capacidad de detectar, priorizar, investigar y responder a las amenazas de forma rápida y precisa.

[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 de Security Hub, CyberGRC proporciona una mayor visibilidad de estos riesgos, para que pueda 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, por lo que puede obtener una visión centralizada de la seguridad junto con la telemetría del rendimiento en el contexto de todo su conjunto.

[AWS Enlace a Marketplace](#)

[Documentación de socios](#)

PagerDuty – PagerDuty

Tipo de integración: Recibir

La PagerDuty La plataforma de gestión de operaciones digitales permite a los equipos mitigar de forma proactiva los problemas que afectan a los clientes al convertir automáticamente cualquier señal en información y acción adecuadas.

AWS los usuarios pueden usar la PagerDuty conjunto de AWS integraciones para escalar sus entornos AWS e híbridos con confianza.

Cuando se combina con alertas de seguridad agrupadas y organizadas de Security Hub, PagerDuty permite a los equipos automatizar su proceso de respuesta a las amenazas y configurar rápidamente acciones personalizadas para evitar posibles problemas.

PagerDuty los usuarios que están llevando a cabo un proyecto de migración a la nube pueden migrar rápidamente y, al mismo tiempo, reducir el impacto de los problemas que se producen a lo largo del 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 organización, automatización y respuesta (SOAR) de seguridad que se integra con toda su gama de productos de seguridad para acelerar la respuesta a los 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 la integración con Security Hub recopila información sobre amenazas y la envía al VM-Series el firewall de última generación es 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 proporciona servicios de seguridad gestionados además de los productos de AWS seguridad nativos para una supervisión ininterrumpida mediante Rackspace SOC, análisis avanzados y corrección de amenazas.

[Enlace al producto](#)

Rapid7 – InsightConnect

Tipo de integración: Recibir

Rapid7 InsightConnect es una solución de coordinación y automatización de la seguridad que permite a su equipo optimizar SOC las operaciones con poco o ningún código.

[Enlace al producto](#)

[Documentación de socios](#)

RSA – RSA Archer

Tipo de integración: Recibir

RSA Archer La gestión de riesgos de TI y seguridad le permite determinar qué activos son fundamentales para su empresa, establecer y comunicar políticas y estándares de seguridad, detectar y responder a los ataques, identificar y corregir las deficiencias de seguridad y establecer prácticas recomendadas claras de gestión de riesgos de TI.

[Enlace al producto](#)

[Documentación de socios](#)

ServiceNow – ITSM

Tipo de integración: Recibir y actualizar

La ServiceNow la integración con Security Hub permite ver los hallazgos de seguridad del Security Hub en ServiceNow ITSM. También puede configurar ServiceNow para crear automáticamente un incidente o un problema cuando reciba un hallazgo de Security Hub.

Cualquier actualización de estos incidentes y problemas da lugar a actualizaciones de los resultados en Security Hub.

Para obtener una descripción general de la integración y su funcionamiento, vea el vídeo [AWS Security Hub: integración bidireccional con ServiceNow ITSM](#).

[Enlace al producto](#)

[Documentación de socios](#)

Slack – Slack

Tipo de integración: Recibir

Slack es una capa del conjunto de tecnologías empresariales 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 de Security Hub. Envíe sus datos a Splunk para análisis de seguridad avanzados ySIEM.

[Enlace al producto](#)

[Documentación de socios](#)

Splunk – Splunk Phantom

Tipo de integración: Recibir

Con el Splunk Phantom aplicación para AWS Security Hub, los resultados se envían a Phantom para enriquecer el contexto de forma automática 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 automatizada de modelado de amenazas 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 resultados de Security Hub

Las siguientes integraciones de socios de terceros envían y reciben resultados de Security Hub.

Caveonix – Caveonix Cloud

Tipo de integración: Enviar y recibir

ProductoARN: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

La Caveonix La plataforma basada en 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, 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

ProductoARN: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodian permite gestionar bien a los usuarios en la nube. Lo simple YAML DSL permite definir reglas fácilmente para crear una infraestructura de nube bien gestionada, segura y rentable.

[Enlace al producto](#)[Documentación de socios](#)

DisruptOps, Inc. – DisruptOPS

Tipo de integración: Enviar y recibir

ProductoARN: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

La DisruptOps La plataforma de operaciones de seguridad ayuda a las organizaciones a mantener las mejores prácticas de seguridad en la nube mediante el uso de barreras automatizadas.

[Enlace al producto](#)[Documentación de socios](#)

Kion

Tipo de integración: Enviar y recibir

Producto: ARN `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion (anteriormente cloudtamer.io) es una solución completa de gobierno de la nube para. AWSKion ofrece 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

ProductoARN: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbot garantiza que su infraestructura de nube sea segura, compatible, escalable y optimizada en cuanto a costes.

[Enlace al producto](#)

[Documentación de socios](#)

Integración de Security Hub a productos personalizados

Además de los resultados generados por los servicios de AWS integrados y los productos de terceros, AWS Security Hub puede consumir los resultados generados por otros productos de seguridad personalizados.

Puede enviar estos resultados a Security Hub mediante la operación [BatchImportFindings](#) de la API de Security Hub. Puede utilizar la misma operación para actualizar los resultados de los productos personalizados que ya ha enviado a Security Hub.

Al configurar la integración personalizada, utilice las [directrices y listas de comprobación](#) que se proporcionan en la Guía de integración de socios de Security Hub.

Requisitos y recomendaciones para las integraciones de productos personalizados

Antes de poder invocar correctamente la operación de la API [BatchImportFindings](#), debe habilitar Security Hub.

También debe proporcionar detalles sobre los resultados del producto personalizado con el [the section called “Formato de los hallazgos”](#). Revise los siguientes requisitos y recomendaciones para las integraciones de productos personalizados:

Configuración del ARN del producto

Al habilitar Security Hub, se genera un nombre de recurso de Amazon (ARN) predeterminado del producto para Security Hub en la cuenta actual.

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

Puede utilizar `BatchImportFindings` para establecer un nombre de empresa y un nombre de producto preferidos para la integración personalizada que envía resultados a Security Hub.

Los nombres que especifique sustituyen al nombre de la empresa y el nombre del producto preconfigurados, denominados nombre personal y nombre predeterminado respectivamente, y aparecen en la consola de Security Hub y en el JSON de cada resultado. Consulte [BatchImportFindings para encontrar proveedores](#).

Configuración de los ID de resultados

Debe proporcionar, administrar e incrementar sus propios ID de resultados, utilizando el atributo [Id](#).

Cada nuevo resultado debería tener un ID de resultado único. Si el producto personalizado envía varios resultados con el mismo ID de resultado, Security Hub solo procesa el primer resultado.

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 escaneos Chef InSpec a Security Hub

Puede crear una plantilla de AWS CloudFormation que ejecute un análisis de conformidad de [Chef InSpec](#) y, a continuación, envíe los resultados a Security Hub.

Para obtener más información, consulte [Supervisión continua de la conformidad con Chef InSpec y AWS Security Hub](#).

Envío de vulnerabilidades de contenedores detectadas por Trivy Security Hub

Puede crear una plantilla de AWS CloudFormation que emplee [AquaSecurity Trivy](#) para analizar contenedores en busca de vulnerabilidades y, a continuación, enviar esos resultados sobre vulnerabilidad a Security Hub.

Para obtener más información, consulte [Cómo crear una canalización de CI/CD para el análisis de vulnerabilidades de contenedores con Trivy y AWS Security Hub](#).

Creación y actualización de los resultados en Security Hub

En AWS Security Hub, un hallazgo es un registro observable de un control de seguridad o una detección relacionada con la seguridad.

Un resultado puede provenir de uno de los siguientes orígenes de Security Hub:

- Un control de seguridad de un control habilitado en Security Hub
- Una integración habilitada con otro Servicio de AWS
- Una integración habilitada con un producto de terceros
- Una integración personalizada

Luego de que sea creado un resultado, el proveedor del resultado o un usuario de Security Hub pueden actualizarlo de la siguiente manera:

- El proveedor de búsqueda puede usar el [BatchImportFindings](#) funcionamiento de la API de Security Hub para actualizar la información general sobre un hallazgo. Los proveedores de hallazgos solo pueden actualizar los hallazgos que hayan creado.
- El cliente puede usar la [BatchUpdateFindings](#) funcionamiento de la API Security Hub para actualizar el estado de la investigación sobre un hallazgo. `BatchUpdateFindings` también se puede utilizar en nombre del cliente mediante una herramienta de emisión de tickets, gestión de incidentes, organización, remediación o SIEM.

Los clientes también pueden actualizar los resultados en la consola de Security Hub.

Security Hub normaliza los hallazgos de todas las fuentes en una sintaxis y un formato estándar denominados AWS Security Finding Format (ASFF). Para obtener más información acerca del ASFF, consulte [AWS Formato de búsqueda de seguridad \(ASFF\)](#).

Security Hub elimina automáticamente los resultados que no se hayan actualizado en los últimos 90 días. En concreto, Security Hub retiene un resultado existente en una cuenta durante 90 días después del valor más reciente del campo `UpdatedAt` en el ASFF. El resultado se retiene durante 90 días a partir de esta fecha, incluso si Security Hub está deshabilitado. Después de los 90 días, Security Hub eliminará de forma permanente los resultados de la cuenta. Al buscar proveedores, se puede cambiar el valor del `UpdatedAt` campo mediante el [BatchImportFindings](#) funcionamiento de la API de Security Hub para actualizar un hallazgo.

Si habilita la agregación entre regiones, Security Hub agrega automáticamente los nuevos resultados actualizados de las regiones vinculadas a la región de agregación. Para obtener más información, consulte [Descripción de agregación entre regiones en Security Hub](#).

BatchImportFindings para encontrar proveedores

Los proveedores de resultados utilizan la operación de la API [BatchImportFindings](#) para crear nuevos resultados y actualizar la información sobre los resultados que generaron. No pueden actualizar los resultados que no hayan generado ellos.

Los clientes deben utilizar las herramientas de venta de entradas y las herramientas de SOAR [BatchUpdateFindings](#) para realizar actualizaciones relacionadas con su investigación sobre los resultados de la búsqueda de proveedores. SIEMs Para obtener más información, consulte [the section called “BatchUpdateFindings para clientes”](#).

Cada vez que AWS Security Hub recibe una BatchImportFindings solicitud para crear o actualizar un hallazgo, genera automáticamente un Security Hub Findings - Importedevento 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 para la integración oficial de un socio de Security Hub.

Security Hub solo puede aceptar actualizaciones de resultados para las cuentas que tengan Security Hub habilitado. El proveedor de hallazgos también debe estar habilitado. Si Security Hub está deshabilitado o la integración del proveedor de resultados no está habilitada, los resultados se devuelven a la lista `FailedFindings` con el error `InvalidAccess`.

Determinación de si se debe crear o actualizar un hallazgo

Para determinar si crear o actualizar un hallazgo, Security Hub comprueba el campo ID. Si el valor de ID no coincide con un resultado existente, Security Hub crea un resultado nuevo.

Si ID coincide con un resultado existente, Security Hub comprueba el campo UpdatedAt para la actualización y procede de la siguiente forma:

- Si UpdatedAt en la actualización coincide con UpdatedAt o se produce antes de esto en el resultado existente, entonces Security Hub ignora la actualización.
- Si UpdatedAt en la actualización se produce después de UpdatedAt en el resultado existente, Security Hub actualiza el resultado 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 ignora todo el contenido proporcionado en una solicitud BatchImportFindings 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.

Actualización de los hallazgos con FindingProviderFields

La búsqueda de proveedores tampoco debería utilizarse BatchImportFindings para actualizar los siguientes atributos de nivel superior en el formato de búsqueda AWS de 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 las solicitudes `BatchImportFindings`, Security Hub gestiona los valores de los atributos de nivel superior y de [FindingProviderFields](#) de la siguiente manera.

(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 actualiza el valor del atributo `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 usa el valor para actualizar el atributo `FindingProviderFields`. Sobrescribe cualquier valor existente.

Security Hub actualiza el atributo de nivel superior solo si `BatchUpdateFindings` aún no ha actualizado el atributo.

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 resultado nuevo, Security Hub utiliza el valor `FindingProviderFields` para rellenar tanto el atributo de nivel superior como el atributo correspondiente a `FindingProviderFields`. No utiliza el valor de atributo de nivel superior proporcionado.

Para un resultado existente, Security Hub usa ambos valores. Sin embargo, actualiza el valor del atributo de nivel superior solo si `BatchUpdateFindings` aún no ha actualizado el atributo.

BatchUpdateFindings para clientes

Los clientes de Security Hub y las entidades que actúen en su nombre pueden utilizar la operación [BatchUpdateFindings](#) para actualizar la información relacionada con el procesamiento de un cliente de los resultados de Security Hub a partir de los proveedores de resultados. Un cliente o una herramienta de SIEM, de creación de tickets, de administración de incidentes o de SOAR que funcione en nombre de un cliente puede utilizar esta operación.

No se puede usar `BatchUpdateFindings` para crear nuevos resultados. Se puede utilizar para actualizar hasta 100 resultados a la vez. En su solicitud, especifique qué campos del formato de búsqueda de AWS seguridad (ASFF) desea actualizar.

Cuando Security Hub recibe una `BatchUpdateFindings` solicitud para 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”](#).

`BatchUpdateFindings` no cambia el campo `UpdatedAt` para el resultado. `UpdatedAt` refleja la actualización más reciente del proveedor de resultados.

Campos disponibles para BatchUpdateFindings

Si inició sesión en una cuenta de administrador de Security Hub, puede utilizar BatchUpdateFindings para actualizar los resultados que generó 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

Configurar el acceso a BatchUpdateFindings

Puede configurar políticas AWS Identity and Access Management (de IAM) para restringir el acceso y utilizarlas BatchUpdateFindings para actualizar los campos de búsqueda y los valores de los campos.

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 de resultados y el historial de resultados en Security Hub

En AWS Security Hub, un hallazgo es un registro observable de un control de seguridad o una detección relacionada con la seguridad. Security Hub 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 de resultados y otros detalles de resultados en la consola de Security Hub y mediante programación a través de la API de Security Hub y la AWS CLI.

Para ayudarlo a optimizar su análisis, la consola de Security Hub abre un panel de resultados cuando selecciona un resultado específico. El panel incluye diferentes menús y pestañas para visualizar diferentes detalles de resultados.

Menús de acciones

Desde este menú, puede revisar el JSON completo de un resultado o agregar notas. Un resultado no puede tener más de una nota adjunta a la 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 del resultado. Por ejemplo, puede ver cuándo se creó y actualizó por última vez el hallazgo, en qué cuenta se encuentra y el origen del hallazgo. Para ver los resultados de control, también puedes ver el nombre de la AWS Config regla asociada y un enlace a las instrucciones de corrección en la documentación 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 resultado. En el caso de algunos recursos, incluimos la opción de abrir un recurso y ver directamente 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. La fecha debe estar dentro de los últimos 90 días. Por ejemplo, si hizo un cambio ayer y otro hoy, la instantánea mostrará solo el cambio de hoy. Para ver las entradas anteriores, cambie a la pestaña Historial.

La fila Conformidad se expande para mostrar más detalles. Por ejemplo, en el caso de los controles que incluyen parámetros, puede ver los valores de los parámetros actuales que utiliza Security Hub cuando lleva a cabo controles de seguridad.

Pestaña recursos

En esta pestaña se proporcionan detalles sobre los recursos que intervienen en un resultado. Si has iniciado sesión en la cuenta propietaria de un recurso, puedes ver el recurso en la Servicio de AWS consola correspondiente. Si no eres el propietario de un recurso, la consola muestra el Cuenta de AWS ID del propietario.

La fila Detalles muestra los detalles específicos del recurso sobre el hallazgo al mostrar el [ResourceDetails](#) sección del JSON de búsqueda.

La fila Etiquetas muestra la información clave y el valor de las etiquetas de los recursos involucrados en un resultado. Recursos [compatibles con el GetResources se puede AWS Resource Groups etiquetar el funcionamiento](#) de la API de etiquetado. Security Hub llama a esta operación a través del [rol vinculado al servicio](#) cuando procesa hallazgos nuevos o actualizados y recupera las etiquetas de recursos si el Resource . Id campo AWS Security Finding Format (ASFF) se rellena con el ARN del recurso. AWS Security Hub ignora el recurso IDs no válido. Para obtener más información sobre la inclusión de etiquetas de recursos en los resultados, consulte [Tags](#).

Pestaña de historial de resultados

Esta pestaña hace un seguimiento del historial de un resultado en los últimos 90 días. El historial de resultados está disponible para los resultados activos y archivados. Este proporciona un registro inmutable de los cambios realizados en un resultado a lo largo del tiempo, incluyendo qué campo del Formato de resultados de seguridad de AWS (ASFF) cambió, cuándo se produjo el cambio y qué usuario lo realizó. Los cambios más recientes se muestran primero. Si inició sesión en una cuenta de administrador de Security Hub, el historial de resultados que se muestra pertenece a la cuenta de administrador y a todas las cuentas de los miembros.

El historial de resultados incluye los cambios que un usuario realizó de forma manual o automática a través de [las reglas de automatización de Security Hub](#). Sin embargo, el historial de resultados no incluye los cambios en los campos de fecha y hora de nivel superior, como `CreatedAt` y `UpdatedAt`.

Pestaña de amenazas

Esta pestaña incluye datos del [Action](#), [Malware](#), y [ProcessDetails](#) objetos de la ASFF, incluidos el tipo de amenaza y si un recurso es el objetivo o el actor. Este objeto normalmente se aplica a las búsquedas que se originan en Amazon GuardDuty.

Pestaña de vulnerabilidades

En esta pestaña se muestran los datos del [Vulnerability](#) objeto de la ASFF, incluso si hay vulnerabilidades o correcciones disponibles asociadas a un hallazgo. Este objeto normalmente se aplica a los resultados que se originan en Amazon Inspector.

Las filas de cada pestaña incluyen una opción de copia o filtro. Por ejemplo, si está en el panel de un resultado 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 selecciona Mostrar todos los resultados con este valor, se filtra la lista de búsquedas para que solo muestre los resultados con el mismo estado del flujo de trabajo.

Consulte la siguiente sección para saber cómo acceder a estos detalles para obtener un resultado.

Instrucciones para revisar los detalles y el historial de los resultados

Elija el método que prefiera y siga estos pasos para visualizar los detalles de los resultados en Security Hub.

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 entre regiones](#).

Security Hub console

Revisión de los detalles y el historial de resultados (consola)

1. Abra la AWS Security Hub consola en. <https://console.aws.amazon.com/securityhub/>
2. Para mostrar una lista de resultados, lleve a cabo una de las siguientes acciones:
 - En el panel de navegación de Security Hub, elija Resultados. Agregue los filtros de búsqueda necesarios para reducir la lista de resultados.
 - En el panel de navegación de Security Hub, elija Información. Elija una información. A continuación, en la lista de resultados, seleccione un resultado de información.
 - En el panel de navegación de Security Hub, elija Integraciones. Seleccione Ver los resultados de una integración.
 - En el panel de navegación de Security Hub, seleccione Controles.
3. Seleccione un título de resultados.
4. En el panel de resultados, realice una de las siguientes acciones:
 - Seleccione el menú Acciones para realizar una acción en relación con el resultado.
 - Seleccione el menú Investigar para investigar el resultado en Amazon Detective.
 - Seleccione una pestaña para ver más detalles sobre el resultado.

Note

Si te integras con una cuenta de miembro de la organización AWS Organizations y la cuenta en la que has iniciado sesión es una cuenta de miembro, el panel de búsqueda incluirá el nombre de la cuenta. En el caso de las cuentas de miembros que se invitan manualmente y no mediante Organizations, el panel de resultados solo incluye el ID de la cuenta.

Security Hub API

Revisar los detalles y el historial de los resultados (API)

Utilizar [GetFindings](#) funcionamiento de la API de Security Hub o, si está utilizando la AWS CLI, ejecute la [get-findings](#) comando

Puede proporcionar uno o varios valores para el parámetro `Filters` para restringir los resultados que quiera 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.

Si activó la [agregación entre regiones](#) e invoca esta operación desde la región de agregación, los resultados incluyen los resultados de la agregación y de las regiones vinculadas.

El siguiente comando de la CLI recupera los resultados que coinciden con los filtros proporcionados y los ordena de forma descendente del 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 búsquedas, utilice la [GetFindingHistory](#) operación. 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 más información sobre estos campos, consulte [AwsSecurityFindingIdentifier](#). Solo puedes obtener el historial de un hallazgo por solicitud.

El siguiente comando de la CLI recupera el historial del resultado 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-  
EXAMPLE11111",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

Revisar los detalles de la búsqueda (PowerShell)

Utilice el cmdlet `Get-SHUBFinding`.

Si lo desea, rellene el parámetro `Filter` para restringir las conclusiones que quiera recuperar.

El siguiente cmdlet recupera los resultados que coinciden con los filtros proporcionados

```
Get-SHUBFinding -Filter @{AwsAccountId =  
[Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =  
"XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =  
"EQUALS"; Value = 'FAILED'}}
```

Note

Cuando filtra los resultados por `CompanyName` o `ProductName`, Security Hub utiliza los valores que forman parte del objeto `ProductFields` del ASFF. Security Hub no utiliza el nivel superior ni los campos `CompanyName` y `ProductName`.

Filtrar los resultados en Security Hub

AWS Security Hub genera sus propios resultados a partir de los controles de seguridad y recibe los resultados de los productos integrados. Puede mostrar una lista de los resultados en las páginas Hallazgos, Integraciones e Información de la consola 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 de la consola de Security Hub se filtran en función de `Workflow.Status` los 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 también archiva automáticamente los resultados 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 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 mostrará los resultados que coincidan con estos dos criterios.

Security Hub aplica OR la lógica a los filtros que utilizan el mismo atributo pero valores diferentes. Por ejemplo, si añades `Amazon Inspector` como valores de filtro para el nombre del producto, Security Hub mostrará las conclusiones generadas por `Amazon GuardDuty` o por `Amazon Inspector`.

Para añadir filtros a una lista de resultados (consola)

1. Abra la AWS Security Hub consola 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

Puede agrupar las conclusiones en AWS Security Hub 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 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 muestra la lista de resultados coincidentes para ese valor.

Para agrupar los resultados en una lista de resultados (consola)

1. Abra la AWS Security Hub consola 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 de flujo de trabajo de los resultados de Security Hub

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 un resultado individual. No afecta a la generación de nuevos resultados. Por ejemplo, establecer el estado del flujo de trabajo de un hallazgo como SUPPRESSED o RESOLVED no AWS Security Hub impide que se genere un nuevo hallazgo para el mismo problema.

El estado de flujo de trabajo puede tener los siguientes valores:

NEW

Es el estado inicial de un resultado antes de revisarlo.

Los hallazgos que se obtienen de forma integrada Servicios de AWS, por ejemplo AWS Config, tienen NEW su estado inicial.

Security Hub también restablece el estado del flujo de trabajo de NOTIFIED o RESOLVED a 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.

NOTIFIED

Indica que informó 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.

SUPPRESSED

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.

RESOLVED

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 resultados de los controles, si `Compliance.Status` es PASSED, Security Hub establece automáticamente el estado del flujo de trabajo en RESOLVED.

Configuración del estado de flujo de trabajo de los resultados

Elija el método que prefiera y siga los pasos para configurar el estado del flujo de trabajo de uno o más resultados.

Para actualizar automáticamente el estado del flujo de trabajo de resultados específicos, consulte [Descripción de las reglas de automatización en Security Hub](#).

Security Hub console

Cómo configurar el estado de flujo de trabajo de los resultados

1. Abra la AWS Security Hub consola 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 de Security Hub, elija Resultados.
 - En el panel de navegación de Security Hub, elija Información. Elija una información. A continuación, en la lista de resultados, seleccione un resultado de información.

- En el panel de navegación de Security Hub, elija Integraciones. Seleccione Ver los resultados de una integración.
 - En el panel de navegación de Security Hub, elija Estándares de seguridad. Seleccione Ver resultados para ver una lista de controles. A continuación, seleccione un control para ver una lista de los resultados de ese control.
3. En la lista de resultados, seleccione la casilla de verificación de cada resultado que desee actualizar.
 4. En la parte superior de la lista, en Estado del flujo de trabajo, elija el estado.
 5. En el cuadro de diálogo Definir el estado del flujo de trabajo, incluya una nota opcional que indique el motivo de la actualización del estado del flujo de trabajo. Seleccione Establecer estado.

Security Hub API

invoque la API [BatchUpdateFindings](#). Proporcione el ID de resultado y el ARN del producto que generó el resultado. Puede obtener estos detalles invocando la API [GetFindings](#).

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 de [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"
```

Envío de los resultados de Security Hub a una acción personalizada

Puedes crear acciones AWS Security Hub personalizadas para automatizar Security Hub con Amazon EventBridge. En el caso de las acciones personalizadas, el tipo de evento es Security Hub Findings - Custom Action.

Para obtener más información y pasos detallados sobre cómo crear acciones personalizadas, consulte [the section called “Respuesta y corrección automatizadas”](#).

Después de configurar una acción personalizada, puede enviarle hallazgos.

Cómo enviar resultados a una acción personalizada (consola)

1. Abre la AWS Security Hub consola 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 de Security Hub, elija Resultados.
 - En el panel de navegación de Security Hub, elija Información. Elija una información. A continuación, en la lista de resultados, seleccione un resultado de información.
 - En el panel de navegación de Security Hub, elija Integraciones. Seleccione Ver los resultados de una integración.
 - En el panel de navegación 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 consume y agrega los hallazgos de productos integrados Servicios de AWS y de terceros. Security Hub 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 AWS de seguridad (ASFF). El formato se deriva del [Esquema JSON](#). Elija el nombre de un objeto vinculado para ver un ejemplo de la resultado de ese objeto. Puede comparar los resultados de Security Hub con los recursos y ejemplos que se muestran aquí para ayudarle a interpretarlas.

Para ver las descripciones de los atributos del ASFF de nivel superior requeridos, consulte [the section called "Atributos de nivel superior necesarios del ASFF"](#).

Para ver las descripciones de los atributos del ASFF de nivel superior opcionales, consulte [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"],
  "CreateDate": "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",
  "CreateDate": "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"
  }],
  "PropogatingVgwSet": [],
  "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

Security Hub ofrece dos tipos de consolidación:

- Vista de controles consolidada (siempre activa; no se puede desactivar): cada control tiene un único identificador en todos los estándares. La página Controles de la consola de Security Hub muestra todos los controles de todos los estándares.
- Resultados de control consolidados (se pueden activar o desactivar): cuando los resultados de control consolidados están activados, Security Hub produce un único resultado para un control de seguridad, incluso cuando un control se comparte en varios estándares. El objetivo es reducir el ruido de detección. Los resultados de control consolidados están activados de forma predeterminada si habilitó Security Hub a partir del 23 del febrero de 2023. De lo contrario, se encuentra desactivada de forma predeterminada. Sin embargo, los resultados de control consolidados solo están activados en las cuentas de los miembros de Security Hub si están activados en la cuenta de administrador. Si la característica está desactivada en la cuenta de administrador, se desactivará en las cuentas de los miembros. Para obtener instrucciones sobre cómo activar esta característica, consulte [Resultados de control consolidados](#).

Ambas funciones incorporan cambios para controlar el resultado de campos y valores en [AWS Formato de búsqueda de seguridad \(ASFF\)](#). Esta sección resume dichos cambios.

Vista de controles consolidada: cambios en ASFF

La característica de vista de controles consolidada introdujo los siguientes cambios para controlar el resultado de campos y valores en el ASFF.

Si sus flujos de trabajo no se basan en los valores de estos campos de resultado de controles, no es necesario realizar ninguna acción.

Si tiene flujos de trabajo que se basan en los valores específicos de estos campos de resultado de controles, actualice los flujos de trabajo para usar los valores actuales.

Campo de ASFF	Valor de muestra antes de la vista de controles consolidados	Valor de muestra después de la vista de controles consolidados, más una descripción del cambio
Cumplimiento. 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.
Cumplimiento. AssociatedStandards	No aplicable (campo nuevo)	<pre> [{" StandardsId «:" standards/aws-foundational-security-best-practices/v /1.0.0 «} </pre>

Campo de ASFF	Valor de muestra antes de la vista de controles consolidados	Valor de muestra después de la vista de controles consolidados, más una descripción del cambio
		Muestra en qué estándares está activado un control.
ProductFields. ArchivalReasons. ----SEP----:0/ Descripción	No aplicable (campo nuevo)	<p>“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”.</p> <p>Describe por qué Security Hub ha archivado los resultados existentes.</p>
ProductFields. ArchivalReasons. ----sep----:0/ ReasonCode	No aplicable (campo nuevo)	<p>“CONSOLIDATED_CONTROLS_FINDINGS_UPDATE”</p> <p>Explica el motivo por el que Security Hub ha archivado los resultados existentes.</p>

Campo de ASFF	Valor de muestra antes de la vista de controles consolidados	Valor de muestra después de la vista de controles consolidados, más 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 de PCI DSS de AWS Security Hub».	«Para obtener instrucciones sobre cómo corregir este problema, consulte la documentación de controles del AWS Security Hub». 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 activa los resultados de control consolidados, es posible que se vea afectado por los siguientes cambios en el control del resultado de campos y valores en ASFF. Estos cambios se suman a los cambios descritos anteriormente para la vista de controles consolidados.

Si sus flujos de trabajo no se basan en los valores de estos campos de resultado de controles, no es necesario realizar ninguna acción.

Si tiene flujos de trabajo que se basan en los valores específicos de estos campos de resultado de controles, actualice los flujos de trabajo para usar los valores actuales.

Note

La [respuesta de seguridad automatizada de la AWS versión 2.0.0](#) respalda las conclusiones de control consolidadas. Si usa esta versión de la solución, puede mantener sus flujos de trabajo al activar los resultados de control consolidados.

Campo de ASFF	Ejemplo de valor antes de activar los resultados de control consolidados	Ejemplo de valor después de activar los resultados del control consolidado y la descripción del cambio
GeneratorId	aws-foundational-security-best-1-practices/v/1.0.0/Config	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	arn:aws:securityhub: eu-central-1:123456789012: security - 6d6a26-a156-48f0-9403-115983e5a956 control/iam.9/finding/ab

Campo de ASFF	Ejemplo de valor antes de activar los resultados de control consolidadas	Ejemplo de valor después de activar los resultados del control consolidado y la descripción del cambio
	subscription/pci-dss/v/3.2.1/PCI.IAM.5/finding/ab	Este campo ya no hace referencia a un estándar.
ProductFields.ControlId	PCI. EC22.	<p>Eliminado. En su lugar, consulte <code>Compliance.SecurityControlId</code>.</p> <p>Este campo se ha eliminado en favor de un único identificador de control independiente del estándar.</p>
ProductFields.RuleId	1.3	<p>Eliminado. En su lugar, consulte <code>Compliance.SecurityControlId</code>.</p> <p>Este campo se ha eliminado en favor de un único identificador de control independiente del estándar.</p>
Descripción	Este control PCI DSS comprueba si AWS Config está activado en la cuenta corriente y en la región.	<p>Este AWS control comprueba si AWS Config está activado en la cuenta corriente y la región.</p> <p>Este campo ya no hace referencia a un estándar.</p>

Campo de ASFF	Ejemplo de valor antes de activar los resultados de control consolidadas	Ejemplo de valor después de activar los resultados del control consolidado y la descripción del cambio
Gravedad	<pre> “Severity”: { “Product”: 90, “Label”: “CRÍTICO”, “Normalized”: 90, “Original”: “CRÍTICO” } </pre>	<pre> “Severity”: { “Label”: “CRÍTICO”, “Normalized”: 90, “Original”: “CRÍTICO” } </pre> <p>Security Hub ya no utiliza el campo Producto para describir la gravedad de un resultado.</p>
Tipos	<pre> ["Software y configuración Checks/Industry and Regulatory Standards/PCI -DSS"] </pre>	<pre> ["Comprobaciones de software y configuración/Normas industriales y reglamentarias"] </pre> <p>Este campo ya no hace referenci a a un estándar.</p>
Conformidad. RelatedRequirements	<pre> ["PCI DSS 10.5.2", “PCI DSS 11.5”, « AWS Fundamentos de la CEI 2.5”] </pre>	<pre> ["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”] </pre> <p>Este campo muestra los requisitos relacionados en todos los estándares habilitados.</p>

Campo de ASFF	Ejemplo de valor antes de activar los resultados de control consolidadas	Ejemplo de valor después de activar los resultados del control consolidado y la descripción del cambio
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 activan los resultados de control consolidados.
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 activan los resultados de control consolidados.
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>standards/aws-foundational-security-best-practices/arn:aws:securityhub:::/1.0.0</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 genera un resultado para un control 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> .

Campo de ASFF	Ejemplo de valor antes de activar los resultados de control consolidadas	Ejemplo de valor después de activar los resultados del control consolidado y la descripción del cambio
ProductFields.StandardsGuideSubscriptionArn	arn:aws:securityhub:us-east-2:123456789012:/1.2.0 subscription/cis-aws-foundations-benchmark/v	Eliminado. Security Hub genera un resultado para un control de seguridad en todos los estándares.
ProductFields.StandardsSubscriptionArn	arn:aws:securityhub:us-east-1:123456789012:/1.0.0 subscription/aws-foundational-security-best-practices/v	Eliminado. Security Hub genera un resultado para un control de seguridad en todos los estándares.
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 activa los [resultados de control consolidados](#), Security Hub genera un resultado para todos los estándares y archiva los resultados originales (resultados separados para cada estándar). Para ver los resultados archivados, puede visitar la página Conclusiones de la consola de Security Hub con el filtro Estado del registro establecido en ARCHIVADO o utilizar la acción de la API de [GetFindings](#). Las actualizaciones que haya realizado en las conclusiones originales en la consola de Security Hub o mediante la [BatchUpdateFindings](#) API no se conservarán en las nuevas conclusiones (si es necesario, puede recuperar estos datos consultando las conclusiones archivadas).

Campo de ASFF proporcionado por el cliente	Descripción del cambio tras activar 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.
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.

Genera las IDs conclusiones antes y después de activar el control consolidado

Esta es una lista de los cambios en la ID del generador para los controles al activar los resultados de control consolidados. Se aplican a los controles que Security Hub admitía a partir del 15 de febrero de 2023.

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
arn:aws:securityhub:::/1.1 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	control de seguridad/ CloudWatch .1

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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.
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	securitycontrol/ CloudWatch .10
arn:aws:securityhub::: /3.11 ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule	security-control/ CloudWatch 1.1

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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.

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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.

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
aws-foundational-security-best-practices/v/1.0.0/EC 2.25	control de seguridad/ .25 EC2
aws-foundational-security-best-1practices/v/1.0.0/ECR.	security-control/ECR.1
aws-foundational-security-best-practices/v/1.0.0/ECR 2.	security-control/ECR.2
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-12practices/v/1.0.0/ECS	security-control/ECS.12
aws-foundational-security-best-2practices/v/1.0.0/ECS.	security-control/ECS.2
aws-foundational-security-best-practices/v/1.0.0/ECS 3.	security-control/ECS.3
aws-foundational-security-best-4practices/v/1.0.0/ECS.	security-control/ECS.4
aws-foundational-security-best-5practices/v/1.0.0/ECS.	security-control/ECS.5
aws-foundational-security-best-8practices/v/1.0.0/ECS.	security-control/ECS.8

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
aws-foundational-security-best- 1practices/ v/1.0.0/EFS.	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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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.

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
aws-foundational-security-best-practices/v/1.0.0/RDS 1.0	security-control/RDS.10
aws-foundational-security-best-practices/v/1.0.0/RDS .11 practices/	security-control/RDS.11
aws-foundational-security-best-practices/v/1.0.0/RDS 1.2 practices/	security-control/RDS.12
aws-foundational-security-best-practices/v/1.0.0/RDS 1.3 practices/	security-control/RDS.13
aws-foundational-security-best-practices/v/1.0.0/RDS 1.4 practices/	security-control/RDS.14
aws-foundational-security-best-practices/v/1.0.0/RDS 1.5 practices/	security-control/RDS.15
aws-foundational-security-best-practices/v/1.0.0/RDS 1.6 practices/	security-control/RDS.16
aws-foundational-security-best-practices/v/1.0.0/RDS 1.7 practices/	security-control/RDS.17
aws-foundational-security-best-practices/v/1.0.0/RDS .18 practices/	security-control/RDS.18
aws-foundational-security-best-practices/v/1.0.0/RDS 1.9 practices/	security-control/RDS.19
aws-foundational-security-best-practices/v/1.0.0/RDS. 2practices/	security-control/RDS.2
aws-foundational-security-best-practices/v/1.0.0/RDS 2.0	security-control/RDS.20

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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 AI.1	control de seguridad/ AI.1 SageMaker
aws-foundational-security-best-practices/v/1.0.0/SageMaker AI.2	control de seguridad/ AI.2 SageMaker
aws-foundational-security-best-practices/v/1.0.0/SageMaker AI.3	control de seguridad/ AI.3 SageMaker
aws-foundational-security-best-practices/v/1.0.0/SecretsManager.1	control de seguridad/ .1 SecretsManager
aws-foundational-security-best-practices/v/1.0.0/SecretsManager.2	control de seguridad/ .2 SecretsManager
aws-foundational-security-best-practices/v/1.0.0/SecretsManager.3	control de seguridad/ 3SecretsManager.
aws-foundational-security-best-practices/v/1.0.0/SecretsManager.4	control de seguridad/ .4SecretsManager.

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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.
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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 SageMaker AI.1	control de seguridad/AI.1 SageMaker
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
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/ .4 APIGateway
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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/ .4 AutoScaling
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
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/ .4 CloudTrail
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/ .4 CodeBuild

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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.

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
service-managed-aws-control- tower/v/1.0.0/EC 2.18	control de seguridad/ .18 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.19	control de seguridad/ .19 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.20	control de seguridad/ .20 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.21	control de seguridad/ 2.1 EC2
service-managed-aws-control- tower/v/1.0.0/EC 2.22	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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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- .10 tower/v/1 .0.0/ECS	security-control/ECS.10
service-managed-aws-control- .12 tower/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- tower/v/1.0.0/ EFS 2.	security-control/EFS.2
service-managed-aws-control- tower/v/1.0.0/ EFS 3.	security-control/EFS.3
service-managed-aws-control- 4tower/v/1.0.0/ EFS.	security-control/EFS.4

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
service-managed-aws-control- 2tower/v/1.0.0/ EKS.	security-control/EKS.2
service-managed-aws-control- tower/v/1.0.0/ ELB 2.	security-control/ELB.2
service-managed-aws-control- tower/v/1.0.0/ ELB 3.	security-control/ELB.3
service-managed-aws-control- 4tower/v/1.0.0/ ELB.	security-control/ELB.4
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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/ .4 NetworkFirewall
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
service-managed-aws-control- tower/v/1.0.0/S3.6	security-control/S3.6
service-managed-aws-control- tower/v/1.0.0/S3.8	security-control/S3.8
service-managed-aws-control- tower/v/1.0.0/S3.9	security-control/S3.9
service-managed-aws-control- tower/v/1.0.0/S3.12	security-control/S3.12
service-managed-aws-control- 3,13 tower/v/1.0.0/S	security-control/S3.13
service-managed-aws-control- AI.1 tower/v/1.0.0/SageMaker	control de seguridad/ AI.1 SageMaker
service-managed-aws-control- 1tower/v/1.0.0/SecretsManager.	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/ .4 SecretsManager
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

GeneratorID antes de activar los resultados de control consolidados	GeneratorID después de activar los resultados de control consolidados
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
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 Security Hub muestra los títulos de control IDs y control de seguridad independientes del estándar, independientemente de si los hallazgos de control consolidados están activados o desactivados en su cuenta. Sin embargo, los resultados de Security Hub contienen títulos de control específicos del estándar (para PCI y CIS v1.2.0) si los resultados de control consolidados están desactivados en su cuenta. Si los resultados de control consolidados están desactivados en su cuenta, los resultados de Security Hub contienen el identificador de control específico del estándar y el identificador del control de seguridad. Para obtener más información sobre cómo la consolidación impacta en los resultados de control, consulte [Ejemplos de resultados de control en Security Hub](#).

En el caso de los controles que forman parte de [Service-Managed Standard](#): cuando los resultados de control consolidados están activados AWS Control Tower, el prefijo CT. se elimina del identificador y del título del control.

Para deshabilitar un control de seguridad en Security Hub, debe deshabilitar todos los controles estándar que correspondan al control de seguridad. En la siguiente tabla se muestra el mapeo del control de seguridad y las titulaciones con los controles IDs y títulos específicos del estándar. IDs IDs y los títulos de los controles que pertenecen al estándar AWS Foundational Security Best Practices v1.0.0 (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, [descárguelos 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 métrica 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

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
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 Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte	[IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte
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

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
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
CIS v1.2.0	2.1 Asegúrese de que CloudTrail esté habilitado en todas las regiones	[CloudTrail.1] CloudTrail debe habilitarse y configurarse con al menos un registro multirregional 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 del 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] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea 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

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
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 CloudTrail bucket de 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 activado el cifrado en reposo
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 flujo de VPC debe estar habilitado en todas 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 no autorizadas a la API
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)

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
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
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 métrica 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] Asegúrese de que existan un filtro de métrica de registro y una alarma para los cambios de duración de CloudTrail de AWS Config

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
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 autenticación de AWS Management Console
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 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 v1.2.0	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 bucket 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 configuración de AWS Config
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 deberían permitir la entrada desde el 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 deberían permitir la entrada desde el 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	[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
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
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 Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte	[IAM.18] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte
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 métrica 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

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
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
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] Los depósitos de uso general de S3 deberían requerir solicitudes de uso 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 habilitado en todas las regiones	[CloudTrail.1] CloudTrail debe habilitarse y configurarse con al menos un registro multirregional 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 del 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 en el bucket de CloudTrail S3	[CloudTrail.7] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de 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 activado 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 flujo de VPC debe estar habilitado en todas 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] Asegúrese de que existan un filtro de métrica de registro y una alarma para los cambios de duración de CloudTrail de AWS Config

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 autenticación de AWS Management Console
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 bucket 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 configuración de AWS Config
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 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
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 el 0.0.0.0/0 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	[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o 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 controles de ELB estado
PCI DSS v3.2.1	PCI. CloudTrail.1 CloudTrail Los registros deben cifrarse en reposo mediante AWS KMS CMKs	[CloudTrail.2] CloudTrail debe tener activado 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] Debe estar habilitada al menos una CloudTrail ruta
PCI DSS v3.2.1	PCI. CloudTrail.3 La validación del archivo de CloudTrail registro debe estar habilitada	[CloudTrail.4] La validación del 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 métrica 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
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 deberían poder restaurarse públicamente

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
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 o saliente
PCI DSS v3.2.1	PCI. EC24. 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 deberían permitir la entrada desde el 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 flujo de VPC debe estar habilitado en todas VPCs
PCI DSS v3.2.1	PCI. ELBv2.1 Application Load Balancer debe configurarse para redirigir todas las solicitudes HTTP a HTTPS	[ELB.1] Application Load Balancer debe configurarse para redirigir todas las HTTP solicitudes 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 debe 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
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

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
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 para los usuarios de IAM deben tener una duración estricta AWS Config
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
PCI DSS v3.2.1	PCI.lambda.2 Las funciones de Lambda deben estar en una VPC	[Lambda.3] Las funciones lambda deben estar en un VPC

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
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
PCI DSS v3.2.1	Los buckets PCI.S3.5 S3 deberían requerir solicitudes para usar Secure Socket Layer	[S3.5] Los depósitos de uso general de S3 deberían requerir solicitudes de uso SSL

Estándar	Identificador y título del control estándar	Identificador y título del control de seguridad
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 AI.1 Las instancias de Amazon SageMaker AI notebook no deberían tener acceso directo a Internet	[SageMaker.1] Las instancias de Amazon SageMaker AI 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 de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras 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 de Amazon gestionadas 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 gestionarse 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 resultado de controles, no es necesario realizar ninguna acción.

Si sus flujos de trabajo se basan en el formato específico de alguno de los campos de resultado de controles que figuran en las tablas, debe actualizar los flujos de trabajo. Por ejemplo, si creó una regla de Amazon CloudWatch Events que activó una acción para un ID de control específico (por

ejemplo, invocar una AWS Lambda función si el ID del control es igual a CIS 2.7), actualice la regla para usar CloudTrail .2, el Compliance .SecurityControlId campo de ese control.

Si creó [información personalizada](#) con alguno de los campos o valores de resultado de controles que cambiaron, debe actualizar esa información para utilizar los campos o valores actuales.

Atributos de nivel superior necesarios del ASFF

Los siguientes atributos de nivel superior en el formato AWS de búsqueda de seguridad (ASFF) son necesarios para todos los hallazgos en Security Hub. Para obtener más información sobre estos atributos obligatorios, consulte [AwsSecurityFinding](#) en la Referencia de la API de AWS Security Hub .

AwsAccountId

El Cuenta de AWS identificador al que se aplica la conclusión.

Ejemplo

```
"AwsAccountId": "111111111111"
```

CreatedAt

Indica cuándo se creó el posible problema de seguridad detectado por un resultado.

Ejemplo

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

Note

Security Hub borra los resultados al cabo de 90 días desde la última actualización o 90 días después de que se crearan si no hay actualizaciones. Para almacenar los hallazgos durante más de 90 días, puedes configurar una regla en Amazon EventBridge que dirija los hallazgos a tu bucket de S3.

Descripción

Una descripción del hallazgo. Este campo puede ser texto reutilizable no específico o información específica de la instancia del hallazgo.

Para los resultados de control que genera Security Hub, 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 resultados de control que genera Security Hub, este campo no hace referencia a un estándar si se activan los [resultados de control consolidados](#).

Ejemplo

```
"GeneratorId": "security-control/Config.1"
```

Id

El identificador específico del producto para un hallazgo. Para los resultados de control que Security Hub genera, este campo proporciona el nombre de recurso de Amazon (ARN) del resultado.

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 que identifica exclusivamente un producto de resultados de terceros después de que el producto se registre en Security Hub.

El formato de este campo es `arn:partition:securityhub:region:account-id:product/company-id/product-id`.

- Para AWS los servicios que están integrados con Security Hub, `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. AWS los servicios que aún no están integrados con Security Hub 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

El [Resources](#) objeto proporciona un conjunto de tipos de datos de recursos que describen los AWS recursos a los que se refiere el hallazgo.

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 [Severity](#) en la referencia de la API de AWS Security Hub .

Severity es a la vez un objeto de nivel superior en un resultado y está anidado debajo del objeto FindingProviderFields.

Solo la API de [BatchUpdateFindings](#) debe actualizar el valor del objeto Severity de nivel superior de un resultado.

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 solicitud BatchImportFindings de un nuevo resultado solo proporciona Label o solo proporciona Normalized, Security Hub rellena automáticamente el valor del otro campo. Los campos Product y Original también se pueden rellenar.

Si el objeto de nivel superior Finding.Severity está presente, pero Finding.FindingProviderFields no lo está, Security Hub crea el objeto FindingProviderFields.Severity y copia todo el 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 solo debe actualizarse mediante [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/Evasión defensiva
- TTPs/Defense Evasion/CloudTrailStopped

Las categorías de tácticas, técnicas y procedimientos (TTPs) de la siguiente lista se alinean con la Matrix™ [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
 - Atributos de nivel superior necesarios del ASFF
 - TTPs

- Acceso inicial
- Ejecución
- Persistencia
- Escalado de privilegios
- Evasión de defensa
- 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
 - User
 - VM
 - Contenedor
 - Sin servidor
 - Proceso
 - Base de datos
 - Datos
- Identificaciones de información confidencial
 - PII

- Contraseñas

- Cuestiones legales
- Datos financieros
- Seguridad
- Usuarios

Ejemplo

```
"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 operación de la API [BatchUpdateFindings](#). Solo puede actualizarlo utilizando [BatchImportFindings](#).

Ejemplo

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

Note

Security Hub borra los resultados al cabo de 90 días desde la última actualización o 90 días después de que se crearan si no hay actualizaciones. Para almacenar los hallazgos durante más de 90 días, puedes configurar una regla en Amazon EventBridge que dirija los hallazgos a tu bucket de S3.

Atributos de nivel superior opcionales del ASFF

Estos atributos de nivel superior son opcionales en el formato de búsqueda AWS de seguridad (ASFF). Para obtener más información sobre estos atributos, consulte la referencia [AwsSecurityFinding](#) de la AWS Security Hub API.

Acción

El objeto [Action](#) 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

El 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 rellena este atributo automáticamente para cada resultado. 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 de Security Hub para filtrar los resultados por nombre de empresa, se utiliza este atributo. Cuando se utiliza la API de Security Hub para filtrar los resultados por nombre de empresa, se utiliza el atributo `aws/securityhub/CompanyName` en `ProductFields`. Security Hub 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 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 “Actualización de los hallazgos con 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 “Actualización de los hallazgos con 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 información sobre la secuencia de GuardDuty ataque AWS Security Hub, debe tener GuardDuty habilitada la función 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:AROA987654321EXAMPLE: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 resultados envía un nuevo resultado a Security Hub, Security Hub rellena el objeto FindingProviderFields de forma automática si está vacío, en función de los campos de nivel superior correspondientes.

Los proveedores de resultados pueden actualizar FindingProviderFields mediante la operación [BatchImportFindings](#) de la API de Security Hub. Los proveedores de resultados no pueden actualizar este objeto mediante [BatchUpdateFindings](#).

Para obtener más información sobre cómo Security Hub gestiona las actualizaciones desde BatchImportFindings a FindingProviderFields y a los atributos de nivel superior correspondientes, consulte [the section called “Actualización de los hallazgos con 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 de seguridad detectado por un resultado.

Esta marca de tiempo refleja la hora en que se observó por primera vez el evento o la vulnerabilidad. Por lo tanto, puede diferir de la marca de tiempo CreatedAt, que refleja la hora en que se creó este registro de resultados.

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 resultados de seguridad detectó por última vez el posible problema de seguridad detectado por un resultado.

Esta marca de tiempo refleja la hora en que el evento o la vulnerabilidad se observó por última vez o por última vez. 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 proporciona este campo en la primera observación, la marca temporal debe ser la misma que la marca temporal `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 recibe Security Hub un resultado y comienza a procesarlo.

Esto difiere de las marcas de tiempo obligatorias `CreatedAt` y `UpdatedAt`, y se refieren a la interacción del proveedor de resultados con el problema de seguridad y el resultado. La marca de tiempo `ProcessedAt` indica cuándo comienza Security Hub a procesar un resultado. Una vez finalizado el procesamiento, aparece un resultado 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.

En el caso de los resultados generadas por los controles 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 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 a `Archival` se utilizan cuando Security Hub archiva un resultado existente. Por ejemplo, Security Hub archiva los resultados existentes al deshabilitar un control o estándar y al activar o desactivar los [resultados del control consolidado](#).

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 resultados basados en el control, el nombre del producto es Security Hub.

Security Hub rellena este atributo automáticamente para cada resultado. 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 de Security Hub para filtrar los resultados por nombre de producto, se utiliza este atributo.

Cuando utiliza la API de Security Hub para filtrar los resultados por nombre de producto, utiliza el atributo `aws/securityhub/ProductName` en `ProductFields`.

Security Hub 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 archiva automáticamente los resultados basados en el control si el recurso asociado se elimina, el recurso no existe o el control está deshabilitado.

RecordState está diseñado para encontrar proveedores de resultados y solo puede ser actualizado por [BatchImportFindings](#). No puede actualizarlo mediante [BatchUpdateFindings](#).

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 del resultado es NOTIFIED o RESOLVED, Security Hub establece automáticamente el estado del flujo de trabajo como NEW.

Ejemplo

```
"RecordState": "ACTIVE"
```

Región

Especifica Región de AWS desde dónde se generó la búsqueda.

Security Hub rellena este atributo automáticamente para cada resultado. 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 los atributos RelatedFindings, consulte [RelatedFinding](#) en la referencia de la API de AWS Security Hub .

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" }  
]
```

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  
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

la [Threats](#) el objeto proporciona detalles sobre la amenaza detectada por un hallazgo.

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 datos que no se asignen a ningún campo estándar del formato de búsqueda de AWS 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

la [,Vulnerabilities](#)El objeto proporciona una lista de las vulnerabilidades asociadas a un hallazgo.

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 “Configurar el estado del flujo de trabajo”](#).

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"
```

Resources Objeto ASFF

El objeto Resources proporciona información acerca de los recursos implicados en un hallazgo.

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](#)
- [AwsAmazonMQ recursos en ASFF](#)
- [AwsApiGateway recursos en ASFF](#)
- [AwsAppSync recursos en ASFF](#)
- [AwsAthena recursos en ASFF](#)
- [AwsAutoScaling recursos en ASFF](#)
- [AwsBackup recursos en ASFF](#)
- [AwsCertificateManager recursos en ASFF](#)
- [AwsCloudFormation recursos en ASFF](#)

- [AwsCloudFront recursos en ASFF](#)
- [AwsCloudTrail recursos en ASFF](#)
- [AwsCloudWatch recursos en ASFF](#)
- [AwsCodeBuild recursos en ASFF](#)
- [AwsDms recursos en ASFF](#)
- [AwsDynamoDB recursos en ASFF](#)
- [AwsEc2 recursos en ASFF](#)
- [AwsEcr recursos en ASFF](#)
- [AwsEcs recursos en ASFF](#)
- [AwsEfs recursos en ASFF](#)
- [AwsEks recursos en ASFF](#)
- [AwsElasticBeanstalk recursos en ASFF](#)
- [AwsElasticSearch recursos en ASFF](#)
- [AwsElb recursos en ASFF](#)
- [AwsEventBridge recursos en ASFF](#)
- [AwsGuardDuty recursos en ASFF](#)
- [AwsIam recursos en ASFF](#)
- [AwsKinesis recursos en ASFF](#)
- [AwsKms recursos en ASFF](#)
- [AwsLambda](#)
- [AwsMsk recursos en ASFF](#)
- [AwsNetworkFirewall recursos en ASFF](#)
- [AwsOpenSearchService recursos en ASFF](#)
- [AwsRds recursos en ASFF](#)
- [AwsRedshift recursos en ASFF](#)
- [AwsRoute53 recursos en ASFF](#)
- [AwsS3 recursos en ASFF](#)
- [AwsSageMaker recursos en ASFF](#)
- [AwsSecretsManager recursos en ASFF](#)

- [AwsSns recursos en ASFF](#)
- [AwsSqs recursos en ASFF](#)
- [AwsSsm recursos en ASFF](#)
- [AwsStepFunctions recursos en ASFF](#)
- [AwsWaf recursos en ASFF](#)
- [AwsXray recursos en ASFF](#)
- [Container Objeto ASFF](#)
- [Other Objeto ASFF](#)

Atributos de recursos

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

la [DataClassification](#) El campo 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": "da4d66eac431652a4d44d490a00500bded52c97d235b7b4752f9f688566fe6de",
    "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"
```

Tags

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"
```

AwsAmazonMQ recursos en 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"
  }
]
}

```

AwsApiGateway recursos en 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": "n7h1mf",
```

```

"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\": \"${context.accountId}\", \"requestAccountId\": \"${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"
},
"CanarySettings": {

```

```

    "PercentTraffic": 0.0,
    "DeploymentId": "ul73s8",
    "StageVariableOverrides" : [
      "String" : "String"
    ],
    "UseStageCache": false
  },
  "TracingEnabled": false,
  "CreateDate": "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,
}

```

AwsAppSync recursos en 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,
}
```

AwsAthena recursos en 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"
}
```

AwsAutoScaling recursos en 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"
}

```

AwsBackup recursos en 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 realizar una copia de seguridad de sus AWS recursos.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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 `AwsBackupBackupVault`, 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"
  }
}

```

AwsCertificateManager recursos en 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"
}

```

AwsCloudFormation recursos en 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
}
```

AwsCloudFront recursos en 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": "E37HOT42DHPVYH",
  "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
                    ]
                }
            }
        }
    ],
    "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"
}
```

AwsCloudTrail recursos en 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"
}
```

AwsCloudWatch recursos en 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"
}
```

AwsCodeBuild recursos en 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"]
  }
}

```

AwsDms recursos en 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWF1",

```

```

    "DatabaseName": "Test",
    "EndpointArn": "arn:aws:dms:us-east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBNPK6MJQVQVQA",
    "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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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:YDYUOHZIXWKQSUCBMUCQCNY44SJW74VJNB5DFWQ",
  "MigrationType": "cdc",
  "ReplicationInstanceArn": "arn:aws:dms:us-east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4Y0UGIMYJUI",
  "ReplicationTaskIdentifier": "test-task",
  "ReplicationTaskSettings": "{\"Logging\":{\"EnableLogging\":false,
  \"EnableLogContext\":false, \"LogComponents\":[{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"TRANSFORMATION\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"SOURCE_UNLOAD\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"IO\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"TARGET_LOAD\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"PERFORMANCE\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"SOURCE_CAPTURE\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"SORTER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"REST_SERVER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"VALIDATOR_EXT\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"TARGET_APPLY\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"TASK_MANAGER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"TABLES_MANAGER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"METADATA_MANAGER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"FILE_FACTORY\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"COMMON\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT

```

```

\","Id\":"ADDONS\"}, {"Severity\":"LOGGER_SEVERITY_DEFAULT\","Id\":"DATA_STRUCTURE
\"}, {"Severity\":"LOGGER_SEVERITY_DEFAULT\","Id\":"COMMUNICATION\"}, {"Severity
\":"LOGGER_SEVERITY_DEFAULT\","Id\":"FILE_TRANSFER\"}], "CloudWatchLogGroup
\":"null","CloudWatchLogStream\":"null"}, {"StreamBufferSettings\":{"StreamBufferCount
\":"3","CtrlStreamBufferSizeInMB\":"5","StreamBufferSizeInMB\":"8"}, {"ErrorBehavior
\":{"FailOnNoTablesCaptured\":"true","ApplyErrorUpdatePolicy\":"LOG_ERROR",
"FailOnTransactionConsistencyBreached\":"false","RecoverableErrorThrottlingMax\":"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","TTRRecordSettings\":"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:ABR8LB0QB3CZY33F7XV253NAJVBNPK6MJQVQVQA"
}
```

AwsDynamoDB recursos en 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"
}
```

AwsEc2 recursos en 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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/wJalrXUtnFEMI/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 [AwsEc2](#) de `VpcEndpointServiceDetails` 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": {
  "AccepterVpcInfo": {
    "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"
}

```

AwsEcr recursos en 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:a568e5c7a953fbaea2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
  "ImageTags": ["00000000-0000-0000-0000-000000000000"],
  "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"
}
```

```
}
```

AwsEcs recursos en 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": "11111111/
knotejs@sha256:356131c9fef1111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "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": "1111111/
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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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",
}
```

AwsEfs recursos en 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"
  }
}
```


AwsEks recursos en ASFF

Los siguientes son 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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": {},
}
}

```

AwsElasticBeanstalk recursos en 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 .

El siguiente ejemplo muestra el formato AWS de búsqueda de 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"

```

```
}
```

AwsElasticSearch recursos en 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"
  }
}

```

AwsElb recursos en 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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"
}

```

AwsEventBridge recursos en 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": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
  \\\"AllowAllAccountsFromOrganizationToPutEvents\\\",\\\"Effect\\\":\\\"Allow
  \\\",\\\"Principal\\\":\\\"*\\\",\\\"Action\\\":\\\"events:PutEvents\\\",\\\"Resource\\\":
  \\\"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\\\",\\\"Condition
  \\\":{\\\"StringEquals\\\":{\\\"aws:PrincipalOrgID\\\":\\\"o-ki7yjtjv5\\\"}}},{\\\"Sid\\\":
  \\\"AllowAccountToManageRulesTheyCreated\\\",\\\"Effect\\\":\\\"Allow\\\",\\\"Principal\\\":{\\\"AWS\\\":
  \\\"arn:aws:iam::123456789012:root\\\"},\\\"Action\\\":[\\\"events:PutRule\\\",\\\"events:PutTargets
  \\\",\\\"events>DeleteRule\\\",\\\"events:RemoveTargets\\\",\\\"events:DisableRule
  \\\",\\\"events:EnableRule\\\",\\\"events:TagResource\\\",\\\"events:UntagResource\\\",
  \\\"events:DescribeRule\\\",\\\"events>ListTargetsByRule\\\",\\\"events>ListTagsForResource\\\"],
  \\\"Resource\\\":\\\"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\\\",\\\"Condition\\\":
  {\\\"StringEqualsIfExists\\\":{\\\"events:creatorAccount\\\":\\\"123456789012\\\"}}}]}"

```

AwsGuardDuty recursos en 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"
    }
  }
}
```

AwsIam recursos en 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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"
    }
  ]
}
```

AwsKinesis recursos en 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"
  }
}
```

AwsKms recursos en 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",
```



```

    },
    "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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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"
}
```

AwsMsk recursos en 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
  }
}

```

AwsNetworkFirewall recursos en 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 .

El siguiente ejemplo muestra el formato AWS de búsqueda de 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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.

En los ejemplos siguientes se muestra 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

AwsOpenSearchService recursos en 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"
    ],
}
}
```

AwsRds recursos en 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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).

El siguiente ejemplo muestra el formato AWS de búsqueda de 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": [

```

```

    {
      "Ec2SecurityGroupOwnerId": "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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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"  
}
```

AwsRedshift recursos en 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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": "Ja1rXUtnFEMI/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"
    }
  ]
}
```

AwsRoute53 recursos en 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"
    }
  ]
}
```

AwsS3 recursos en ASFF

Los siguientes son 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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-hrzrlukc5m36ft7okagglf3gmwluquuse1b-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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsS3Bucket` objeto. Para ver las descripciones de `AwsS3Bucket` los atributos, consulte [AWSS3 BucketDetails](#) 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",
          "KMSMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
        }
      }
    ]
  }
}

```

AwsS3Object

El objeto `AwsS3Object` proporciona información sobre un objeto de Amazon S3.

El siguiente ejemplo muestra el formato AWS de búsqueda de seguridad (ASFF) del `AwsS3Object` objeto. Para ver las descripciones de `AwsS3Object` los atributos, consulte [AWSS3 ObjectDetails](#) 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_HH11IxPE35P.MELYaYh"
}

```

AwsSageMaker recursos en 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":
"sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-
east-1.sagemaker.aws",
    "VolumeSizeInGB": 5
  }

```

AwsSecretsManager recursos en 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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"
}
```

AwsSns recursos en 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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"
```

```
}
```

AwsSqs recursos en 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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"
}
```

AwsSsm recursos en 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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"
    }
  }
}
```

AwsStepFunctions recursos en 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
  }
}
```

AwsWaf recursos en 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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 de la 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"
}
}

```

AwsXray recursos en 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.

El siguiente ejemplo muestra el formato AWS de búsqueda de 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"
}

```

Container Objeto ASFF

En el siguiente ejemplo, se 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": "11111111/
knotejs@sha256:372131c9fef1111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "Name": "knote",
  "Privileged": true,
  "VolumeMounts": [{
    "Name": "vol-03909e9",
    "MountPath": "/mnt/etc"
  }]
}
```

Other Objeto ASFF

En el siguiente ejemplo, se 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.

Visualizar información en Security Hub

La información en AWS Security Hub es una colección de resultados relacionados. La información puede identificar un área de seguridad específica que requiera atención e intervención. Por ejemplo, una información podría señalar las instancias EC2 que son objeto de resultados que detectan prácticas de seguridad deficientes. 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 ofrece varias informaciones administradas integradas. No puede modificar ni eliminar la información administrada. También puede crear informaciones personalizadas para realizar un seguimiento de problemas de seguridad que son exclusivos de su entorno y uso de AWS.

La página Información en la consola de AWS Security Hub 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 hallazgos administrados, elija Hallazgos gestionados mediante Security Hub.
- 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).

Ver y tomar medidas sobre los hallazgos y resultados del conocimiento

Para cada hallazgo, AWS Security Hub primero determina los resultados que coinciden con los criterios del filtro y utiliza el atributo de agrupación para agrupar los resultados correspondientes.

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 entre 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 de Security Hub, la lista de resultados se ordena de los resultados más coincidentes a los menos coincidentes. Security Hub 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 ID de cuentas principales para los resultados correspondientes
- Tipo de recurso: los cinco tipos de recursos principales para los resultados correspondientes
- ID de recurso: los cinco principales ID de recursos para los resultados correspondientes
- 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 regla de Amazon CloudWatch para el tipo de evento Security Hub Insight Results. 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 console

Para visualizar y adoptar medidas sobre los resultados de la información (consola)

1. Abra la consola de AWS Security Hub en <https://console.aws.amazon.com/securityhub/>.
2. En el panel de navegación, elija Hallazgos.
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 API, AWS CLI

Para visualizar y adoptar medidas sobre los resultados de la información (API, AWS CLI)

Para ver los resultados de la información, utilice la operación [>GetInsightResults](#) de la API de Security Hub. Si utiliza la AWS CLI, ejecute el comando [get-insight-results](#).

Para identificar la información para la que obtener resultados, necesita el ARN de la información. Para obtener los ARN de información personalizada, utilice la operación [GetInsights](#) de la API o el comando [get-insight-results](#).

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)

Puede mostrar la lista de hallazgos de cada resultado en una lista de resultados de la información en la consola de Security Hub.

Para visualizar y tomar medidas sobre los resultados de la información (consola)

1. Abra la consola de AWS Security Hub en <https://console.aws.amazon.com/securityhub/>.
2. En el panel de navegación, elija Hallazgos.
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:

- [Filtrar los resultados en Security Hub](#)
- [Instrucciones para revisar los detalles y el historial de los resultados](#)
- [Configuración del estado de flujo de trabajo de los resultados de Security Hub](#)
- [Envío de los resultados de Security Hub a una acción personalizada](#)

Lista de hallazgos administrados en Security Hub

AWS Security Hub proporciona varios hallazgos administrados.

Los hallazgos administrados de Security Hub no se pueden modificar ni eliminar. 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.

En este momento, Security Hub ofrece los siguientes hallazgos administrados:

1. Recursos de AWS con la mayoría de 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. AMI que está generando la mayor cantidad de resultados

ARN: `arn:aws:securityhub:::insight/securityhub/default/3`

Agrupados por: ID de imagen de instancia EC2

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. Instancias EC2 implicadas en Tácticas, técnicas y procedimientos (TTP) conocidos

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. Entidades principales de AWS 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. Instancias de recursos de AWS que no cumplen las prácticas recomendadas/ estándares 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. Recursos de AWS asociados con posibles filtraciones de datos

ARN: `arn:aws:securityhub:::insight/securityhub/default/7`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con Effects/Data Exfiltration/
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

8. Recursos de AWS asociados a un consumo de recursos no autorizado

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. Instancias EC2 a las que les faltan parches de seguridad para importantes vulnerabilidades

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. Instancias EC2 con comportamiento inusual en 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. Instancias EC2 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. Instancias EC2 que no cumplen los estándares o las prácticas recomendadas 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. Instancias EC2 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. Instancias EC2 asociadas con reconocimiento de adversarios

ARN: `arn:aws:securityhub:::insight/securityhub/default/22`

Agrupados por: ID de recurso

Filtros de resultados:

- El tipo comienza con TTPS/Discovery/Recon
- El tipo de recurso es AwsEc2Instance
- El estado de registro es ACTIVE
- El estado de flujo de trabajo es NEW o NOTIFIED

18. Recursos de AWS que están asociados con 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. Recursos de AWS asociados con 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. Recursos de AWS con intentos de acceso no autorizado

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. Principales instancias EC2 por número de resultados

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. Principales AML por número de hallazgos

ARN: `arn:aws:securityhub:::insight/securityhub/default/32`

Agrupados por: ID de imagen de instancia EC2

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 de AWS Health con la mayor cantidad de resultados

ARN: `arn:aws:securityhub:::insight/securityhub/default/38`

Agrupados por: ID de recurso

Filtros de resultados:

- `ProductName` igual a `Health`

34. Recursos de AWS Config con la mayor cantidad de resultados

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 hallazgos personalizados en Security Hub

Además de la información gestionada por AWS Security Hub, puede crear información personalizada en Security Hub 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, Security Hub aplica la lógica booleana OR a los filtros que utilizan el mismo atributo, pero valores distintos. 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 IAM acceso. 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, la información personalizada se puede utilizar 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 hallazgos personalizados en Security Hub](#).

Elija el método que prefiera y siga los pasos para crear un hallazgo personalizado en Security Hub.

Security Hub console

Para crear un hallazgo personalizado (consola)

1. Abra la consola AWS de Security Hub 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 API

Para crear una información personalizada (API)

1. Para crear una información personalizada, utilice la [CreateInsight](#)funcionamiento del Security HubAPI. Si usa el AWS CLI, ejecute el [create-insightcomando](#)
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 se encuentra en la consola de Security Hub.

Para crear un nuevo hallazgo personalizado a partir de un hallazgo administrado (consola)

1. Abra la consola AWS de Security Hub 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, la información personalizada se puede utilizar 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 hallazgos personalizados en Security Hub](#).

Para editar un hallazgo personalizado, elija el método que prefiera y siga las instrucciones.

Security Hub console

Para editar un hallazgo personalizado (consola)

1. Abra la consola AWS de Security Hub 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 API

Para editar una información personalizada (API)

1. Utilice el [UpdateInsight](#) funcionamiento del Security Hub API. Si usa el AWS CLI ejecute el [update-insight](#) comando
2. Para identificar la información personalizada que desea actualizar, proporcione el nombre del recurso de Amazon de la información (ARN). Para obtener una información personalizada, utilice la [GetInsights](#) operación o la ARN [get-insights](#) comando
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-EXAMPLE11111" --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 la información personalizada, proporcione el nombre del recurso de Amazon de la información (ARN). Para obtener una información personalizada, utilice el `Get-SHUBInsight` cmdlet. ARN
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, la información personalizada se puede utilizar 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 hallazgos personalizados en Security Hub](#).

Para eliminar un hallazgo personalizado, elija el método que prefiera y siga las instrucciones. No puede eliminar un hallazgo administrado.

Security Hub console

Para eliminar un hallazgo personalizado (consola)

1. Abra la consola AWS de Security Hub 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 API

Para eliminar una información personalizada (API)

1. Utilice el [DeleteInsight](#) funcionamiento del Security Hub API. Si usa el AWS CLI ejecute el [delete-insight](#) comando
2. Para identificar la información personalizada que desea eliminar, proporcione la información ARN. Para obtener ARN una visión personalizada, utilice la [GetInsights](#) operación o [get-insights](#) comando

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 la información personalizada, proporcione la información ARN. Para obtener información personalizada, utilice el `Get-SHUBInsight` cmdlet. ARN

Ejemplo

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```


Modificación automática de los resultados de Security Hub y adopción de medidas al respecto

AWS Security Hub dispone de características que modifican de manera automática los resultados y toman medidas en función de las especificaciones.

Security Hub actualmente admite 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 reglas personalizadas de Amazon EventBridge que definan las acciones automáticas que se deben llevar a cabo en función de resultados e información específicos.

Las reglas de automatización son útiles cuando se desea actualizar de manera automática los campos de resultados en formato de resultados de seguridad de AWS (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.

Las reglas de EventBridge son útiles cuando desea tomar medidas fuera de Security Hub con respecto a resultados específicos o enviar resultados específicos a herramientas de terceros para que los corrijan o investiguen más a fondo. Las reglas se pueden utilizar para desencadenar acciones compatibles, como invocar una función AWS Lambda o notificar un tema de Amazon Simple Notification Service (Amazon SNS) acerca de un resultado específico.

Las reglas de automatización tienen efecto antes de se apliquen las reglas de EventBridge. Es decir, las reglas de automatización se desencadenan y actualizan un resultado antes de que EventBridge lo reciba. A continuación, las reglas de EventBridge se aplican al resultado actualizado.

Al configurar automatizaciones para los controles de seguridad, recomendamos filtrar en función del ID del control en vez del título o la descripción. Si bien Security Hub actualiza ocasionalmente los títulos y descripciones de los controles, los ID de los controles permanecen invariables.

Temas

- [Descripción de las reglas de automatización en Security Hub](#)
- [Uso EventBridge para respuesta y remediación automatizadas](#)

Descripción de las reglas de automatización en Security Hub

Puede utilizar las reglas de automatización para actualizar de manera automática los resultados en AWS Security Hub. A medida que se ingieren resultados, Security Hub puede aplicar una variedad de acciones de reglas, como suprimir resultados, 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.

Solo puede crear y administrar reglas de automatización desde una cuenta de administrador de Security Hub.

Las reglas se aplican a los resultados tanto nuevos como actualizados. Puede crear una regla personalizada de cero o utilizar una plantilla de regla proporcionada por Security Hub. 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 Security Hub, puede crear una regla de automatización mediante la definición de uno o más criterios de reglas y una o más acciones de reglas. Cuando un resultado coincide con los criterios definidos, Security Hub aplica las acciones de reglas. Para obtener más información sobre los criterios y acciones disponibles, consulte [Criterios de regla y acciones de regla disponibles](#).

En la actualidad, Security Hub admite un máximo de 100 reglas de automatización para cada cuenta de administrador.

La cuenta de administrador 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 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 Región de AWS lugar 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 Security Hub, Security Hub API o [AWS CloudFormation](#). También puede utilizar un [script de implementación en varias regiones](#).

Crterios 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	Seleccione (consulte los recursos compatibles con 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 [StringFilter](#) en la AWS Security Hub APIReferencia.

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 [AutomationRulesFindingFilters](#) en la AWS Security Hub APIReferencia.

Los siguientes ASFF campos se admiten actualmente como acciones para las reglas de automatización:

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

Para obtener más información sobre ASFF campos específicos, consulte la [sintaxis del formato de búsqueda de AWS seguridad \(ASFF\)](#).

Tip

Si desea que Security Hub deje de generar resultados para un control específico, le recomendamos deshabilitar el control en lugar de utilizar una regla de automatización. Al deshabilitar un control, Security Hub 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. Recomendamos usar reglas de automatización para cambiar los valores de ASFF campos específicos para encontrar resultados que coincidan con los criterios definidos. Para obtener más información sobre cómo deshabilitar controles, consulte [Deshabilitar controles en Security Hub](#).

Resultados que las reglas de automatización evalúan

Una regla de automatización evalúa los hallazgos nuevos y actualizados que Security Hub genera o ingiere a través del [BatchImportFindings](#) operación después de crear la regla. Security Hub actualiza los resultados 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 existentes a través del [BatchImportFindings](#) funcionamiento del Security HubAPI. Las reglas no se activan cuando se actualizan los campos de búsqueda tras la creación de la regla mediante el [BatchUpdateFindings](#) operación. 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.

Cuando crea o edita una regla en la consola de Security Hub, la consola muestra una vista previa 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 vista previa de la consola refleja las conclusiones en su estado final, tal como se mostrarían en una respuesta a la [GetFindings](#) API operación (es decir, después de aplicar las acciones de la regla u otras actualizaciones al hallazgo).

Cómo funciona el orden de las reglas

Al crear reglas de automatización, usted asigna a cada regla un orden. Esto determina el orden en que Security Hub aplica sus reglas de automatización y adquiere importancia cuando varias reglas se relacionan con el mismo resultado o campo de resultado.

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 de Security Hub, Security Hub asigna automáticamente el orden de las reglas según el orden de creación de las mismas. La regla creada más recientemente tiene el valor numérico más bajo de orden de reglas y, por lo tanto, se aplica primero. Security Hub aplica las reglas subsiguientes en orden ascendente.

Al crear una regla a través del Security Hub API o AWS CLI, Security Hub aplica `RuleOrder` primero la regla con el valor numérico más bajo. Luego aplica las reglas subsiguientes en orden ascendente. Si varios resultados tienen el mismo `RuleOrder`, Security Hub aplica primero una regla con un valor anterior del campo `UpdatedAt` (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`

- `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 los resultados de Security Hub que coincidan con los criterios de la regla A. A continuación, se aplican las acciones de la regla B a los resultados 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

Una regla de automatización puede utilizarse para actualizar de manera automática los resultados en AWS Security Hub. Puede crear una regla de automatización personalizada de cero o utilizar una plantilla de regla precompletada en la consola de Security Hub. Para obtener información general sobre cómo funcionan las reglas de automatización, consulte [Descripción de las reglas de automatización en Security Hub](#).

Solo puede crear una regla de automatización a la vez. Para crear varias reglas de automatización, siga los procedimientos de la consola varias veces o llame al comando API o varias veces 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 de Security Hub, Security Hub le muestra una vista previa de los resultados a los que se aplica la regla. La vista previa no es compatible actualmente si los criterios de la regla incluyen un CONTAINS filtro CONTAINS o NOT _. 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.

Crear 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 de Security Hub, abra la AWS Security Hub consola 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 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 muestra una vista previa de los resultados que coinciden 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 de Security Hub. Esto API crea una regla con un nombre de recurso de Amazon específico (ARN).
2. Escriba 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 aplica primero las reglas con un valor numérico más bajo para este parámetro.
5. En el parámetro `RuleStatus`, especifique si desea que Security Hub habilite y comience a aplicar la regla a los resultados 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. En el `Criteria` parámetro, indique los criterios que desea que Security Hub utilice para filtrar sus resultados. 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. En el parámetro `Actions`, indique las acciones que desea que Security Hub realice cuando haya una coincidencia entre un resultado 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 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 de Security Hub, abra la AWS Security Hub consola 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 muestra una vista previa de los resultados que coinciden 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 Crear regla.

Visualización de las reglas de automatización

Las reglas de automatización pueden utilizarse para actualizar automáticamente los resultados en AWS Security Hub. Para obtener información general sobre cómo funcionan las reglas de automatización, consulte [Descripción de las reglas de automatización en Security Hub](#).

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 de resultados y el historial de resultados en Security Hub](#).

Console

Para ver las reglas de automatización (consola)

1. Con las credenciales de administrador de Security Hub, abra la consola de AWS Security Hub 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, ejecute [ListAutomationRules](#) desde la cuenta de administrador de Security Hub. Esta API devuelve los ARN 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 más detalles sobre las reglas, incluyendo los criterios y las acciones de una regla, ejecute [BatchGetAutomationRules](#) desde la cuenta de administrador de Security Hub. Proporcione los ARN de las reglas de automatización cuyos detalles desee obtener.

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

Las reglas de automatización pueden utilizarse para actualizar automáticamente los resultados en AWS Security Hub. Para obtener información general sobre cómo funcionan las reglas de automatización, consulte [Descripción de las reglas de automatización en Security Hub](#).

Tras crear una regla de automatización, el administrador delegado de Security Hub puede editar la regla. Al editar una regla de automatización, los cambios se aplican a los resultados nuevos y actualizados que Security Hub genere o ingiera después de editarse 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 de administrador de Security Hub, abra la consola de AWS Security Hub 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 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

Una regla de automatización puede utilizarse para actualizar de manera automática los resultados en AWS Security Hub. Para obtener información general sobre cómo funcionan las reglas de automatización, consulte [Descripción de las reglas de automatización en Security Hub](#).

Después de crear una regla de automatización, el administrador delegado de Security Hub puede editar la regla.

Si desea mantener los criterios y las acciones de la regla tal como están, pero desea cambiar el orden en que Security Hub aplica una regla de automatización, puede editar solo el orden de la regla. 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 de administrador de Security Hub, abra la consola de AWS Security Hub 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 de Security Hub, Security Hub asigna automáticamente el orden de las reglas según el orden de creación de las mismas. 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. Use la operación [BatchUpdateAutomationRules](#) desde la cuenta de administrador 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 el mismo `RuleOrder`, Security Hub aplica primero una regla con un valor anterior para el campo `UpdatedAt` (es decir, la regla que se editó más recientemente se aplica en último lugar).

Eliminar o desactivar las reglas de automatización

Las reglas de automatización pueden utilizarse para actualizar automáticamente los resultados en AWS Security Hub. Para obtener información general sobre cómo funcionan las reglas de automatización, consulte [Descripción de las reglas de automatización en Security Hub](#).

Al eliminar una regla de automatización, Security Hub la elimina de su cuenta y deja de aplicarla a los resultados. Como alternativa a la eliminación, puede desactivar una regla. Esto retiene la regla para

uso futuro, pero Security Hub no aplicará la regla a ningún resultado coincidente hasta que usted la habilite.

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 de administrador de Security Hub, abra la consola de AWS Security Hub 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. Use la operación [BatchDeleteAutomationRules](#) desde la cuenta de administrador 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-EXAMPLE11111"]' \
--region us-east-1
```

Ejemplos de reglas de automatización en Security Hub

En esta sección se incluye algunos ejemplos de reglas de automatización para casos de uso comunes. Estos ejemplos corresponden a las plantillas de reglas de la AWS Security Hub consola.

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 API solicitud:

```
{
  "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",
      "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 CLI comando:

```

$
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",
"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 API solicitud:

```

{
  "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",
      "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 CLI comando:

```
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",  
"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 resultados de INFORMATIONAL gravedad enviados a Security Hub desde Amazon GuardDuty. La acción de la regla es cambiar el estado del flujo de trabajo de los resultados coincidentes a SUPPRESSED.

Ejemplo de API solicitud:

```

{
  "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 CLI comando:

```

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 AWS Security Hub conclusiones. Security Hub envía los resultados en forma de eventos prácticamente 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 SNS tema de Amazon o una cola de Amazon SQS
- Enviar un hallazgo a una herramienta de gestión y respuesta a incidentes de terceros para la venta de entradasSIEM, el chat o la gestión de incidencias

Security Hub 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 utilizar acciones personalizadas de Security Hub para crear acciones de respuesta y corrección 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 de Security Hub en EventBridge](#)
- [EventBridge formatos de eventos para Security Hub](#)
- [Configuración de una EventBridge regla para los hallazgos de Security Hub](#)
- [Utilizar acciones personalizadas para enviar las conclusiones y los resultados de información a EventBridge](#)

Tipos de eventos de Security Hub en EventBridge

Security Hub utiliza los siguientes tipos de EventBridge eventos de Amazon para integrarse EventBridge.

En el EventBridge panel de control de Security Hub, Todos los eventos incluye todos estos tipos de eventos.

Todos los hallazgos (Security Hub Findings - Imported)

Security Hub envía automáticamente todos los nuevos hallazgos y todas las actualizaciones de los hallazgos existentes EventBridge a Security Hub Findings - Imported eventos. Cada uno Security Hub Findings - Imported del evento contiene un único hallazgo.

Cada [BatchUpdateFindings](#) solicitud [BatchImportFindings](#) desencadena un Security Hub Findings - ImportedEvento .

En el caso de las cuentas de administrador, el feed de eventos EventBridge incluye eventos con los resultados obtenidos tanto en su cuenta como en 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 entre 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 “Configurar una regla para los resultados de Security Hub”](#).

Hallazgos para acciones personalizadas (Security Hub Findings - Custom Action)

Security Hub también envía los resultados asociados a acciones personalizadas a EventBridge as Security Hub Findings - Custom Action eventos.

Esto resulta útil para los analistas que trabajan con la consola de Security Hub y desean enviar un resultado específico, o un pequeño conjunto de resultados, 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 EventBridge evento independiente.

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 `send_to_ticketing`. A continuación EventBridge, se crea una regla que se activa cuando se EventBridge recibe un resultado que incluye el ID de acción `send_to_ticketing` personalizado. La regla incluye lógica para enviar el resultado a su sistema de tickets. A continuación, puede seleccionar los resultados

en Security Hub y utilizar la acción personalizada en Security Hub para enviar manualmente los resultados a su sistema de tickets.

Para ver ejemplos de cómo enviar las conclusiones de Security Hub EventBridge para su posterior procesamiento, consulte [Cómo integrar acciones AWS Security Hub personalizadas PagerDuty](#) y [Cómo habilitar acciones personalizadas AWS Security Hub en el blog AWS Partner Network \(APN\)](#).

Obtenga información sobre los resultados de las acciones personalizadas (Security Hub Insight Results)

También puedes usar acciones personalizadas para enviar conjuntos de resultados de información a EventBridge as Security Hub Insight Resultseventos. Los resultados de información son los recursos que coinciden con una información. Tenga en cuenta que cuando envía los resultados de 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 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

Con la Security Hub Findings - Imported, Security Findings - Custom Action, y Security Hub Insight Results los tipos de eventos utilizan los siguientes formatos de eventos.

El formato del evento es el formato que se utiliza cuando Security Hub envía un evento a EventBridge.

Security Hub Findings - Imported

Security Hub Findings - Importedeventos que se envían desde Security Hub 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/maciekarn:aws:maciek:us-west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/f2893b211841"
    ],
    "detail": {
      "findings": [
        <finding content>
      ]
    }
  }
}

```

<finding content> es el contenido, en JSON formato, de la conclusión 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 con estos eventos, consulte [the section called “Configurar una regla para los resultados de Security Hub”](#).

Security Hub Findings - Custom Action

Security Hub Findings - Custom Action eventos que se envían desde Security Hub 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 JSON formato, de la conclusión 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 con 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 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 los hallazgos de Security Hub

Puedes crear una regla en Amazon EventBridge que defina la acción que se debe realizar cuando un Security Hub Findings - Imported se recibe un evento. Security Hub Findings - Imported los eventos se desencadenan mediante actualizaciones de las [BatchUpdateFindings](#) 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 la [PutRule](#) operación de EventBridge API. Sin embargo, si usa el 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 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 de AWS seguridad (ASFF).

Tip

Al filtrar los resultados de los controles, se recomienda utilizar los `SecurityControlArn` [ASFFcampos SecurityControlId](#) o como filtros, en lugar de `Title` o `Description`. Estos últimos campos pueden cambiar de vez en cuando, mientras que el ID de control y 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 usar 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	<p>En la sección Patrón de eventos, elija una de las siguientes opciones:</p> <ul style="list-style-type: none"> • 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 	

Cómo crear el patrón de eventos con...	Haga lo siguiente...	
	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...	
<p>Un patrón de eventos personalizado</p> <p>(Utilice un patrón personalizado si desea filtrar los resultados en función de atributos que no aparecen en la EventBridge consola).</p>	<ul style="list-style-type: none">En la sección Patrón de eventos, elija Patrones personalizados (JSONeditor) y, a continuación, pegue el siguiente patrón de eventos en el área de texto: <pre data-bbox="690 632 1062 1425">{ "source": ["aws.securityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "<attribute name> ": ["<value1>", "<value2>"] } } }</pre> <ul style="list-style-type: none">Actualice el patrón de eventos para incluir el atributo y los valores del atributo que desee utilizar como filtro. <p>Por ejemplo, para aplicar la regla a los resultados que tengan un estado de</p>	

Cómo crear el patrón de eventos con...	Haga lo siguiente...	
	<p>verificación TRUE_POSITIVE , utilice el siguiente patrón de ejemplo:</p> <pre data-bbox="690 430 1063 1176">{ "source": ["aws.secu rityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "Verifica tionState": ["TRUE_POSITIVE"] } } }</pre>	

- Para los tipos de objetivos, elige un AWS servicio y, para Selecciona un objetivo, elige un objetivo, como un SNS tema o una AWS Lambda función de Amazon. 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 acciones AWS Security Hub personalizadas para enviar hallazgos o resultados de información a Amazon EventBridge, primero debes crear la acción personalizada en Security Hub. 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 usa el nombre del recurso de Amazon (ARN) de la acción personalizada.

Crear una acción personalizada

Al crear una acción personalizada en AWS Security Hub, 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 envía cada hallazgo a EventBridge como un evento.

Elija su método preferido y siga los pasos para crear una acción personalizada.

Console

Cómo crear una acción personalizada en Security Hub (consola)

1. Abra la AWS Security Hub consola 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 la acción Personalizar ARN. Debe utilizarla ARN cuando cree una regla para asociarla a esta acción en EventBridge.

API

Para crear una acción personalizada (API)

Utilizar [CreateActionTarget](#) operación. 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 del 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 puede utilizar la [PutRule](#) API operación de EventBridge API. Sin embargo, si usa el 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. Abra 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. Elige una acción personalizada específica ARNs y añade una acción personalizadaARN.

Si la regla se aplica a varias acciones personalizadas, selecciona Añadir para añadir más acciones personalizadasARNs.

14. Elija Next (Siguiente).

15. En Seleccionar objetivos, elija y configure el objetivo por invocar cuando esta regla coincida.

16. Elija Next (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 Next (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 acciones AWS Security Hub personalizadas y EventBridge reglas de Amazon, puedes enviar las conclusiones y los resultados de las estadísticas EventBridge para su gestión y procesamiento automáticos.

Los eventos se envían EventBridge solo 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 AWS API las llamadas sean efectivas, las implementaciones del código de destino deben cambiar las funciones a las cuentas de los 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 AWS Security Hub consola 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 [Visualización de los detalles de un control](#).
- En Integraciones puede dirigirse a una lista de resultados generada por una de las integraciones habilitadas. Para obtener más información, consulte [Visualizar resultados desde una integración](#).
- En Información, puede dirigirse a una lista de resultados de un resultado de información. Para obtener más información, consulte [Ver y tomar medidas sobre los hallazgos y resultados del conocimiento](#).

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.

Security Hub envía un evento Resultados de Security Hub - Acción personalizada independiente para cada resultado.

Para enviar los resultados de insights a EventBridge (consola)

1. Abra la AWS Security Hub consola 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.

Uso del panel Resumen en Security Hub

En la consola de AWS Security Hub, el panel de control de la página de resumen puede ayudarlo a identificar las áreas de preocupación de seguridad en su AWS entorno, sin necesidad de herramientas de análisis adicionales ni consultas complejas. Puede personalizar el diseño del panel, agregar o eliminar widgets y filtrar los datos para centrarse en áreas de especial interés. También puede guardar los criterios de filtro como un conjunto de filtros para recuperar rápidamente tipos de datos específicos en el futuro.

Si personaliza el panel o filtra los datos, Security Hub guarda automáticamente la configuración para utilizarla posteriormente. Además, la configuración se guarda de forma independiente para cada usuario de su cuenta de Security Hub. Esto significa que los distintos usuarios pueden tener diferentes diseños, widgets y conjuntos de filtros para el panel.

Cada vez que abre el panel Resumen, Security Hub actualiza automáticamente la mayoría de sus datos. Sin embargo, algunos de los datos se actualizan con menos frecuencia. Por ejemplo, las puntuaciones de seguridad y los estados de control se actualizan cada 24 horas.

Si ha configurado una región de agregación entre regiones para Security Hub, los datos del panel incluyen los resultados de la región de agregación y de todas las regiones vinculadas. Si es el administrador delegado de Security Hub de una organización, los datos incluyen los resultados de su cuenta de administrador y de las cuentas de sus miembros. Si lo desea, puede filtrar los datos por cuenta. Si tiene una cuenta de miembro o una cuenta independiente, los datos incluyen únicamente los resultados de su cuenta.

Widgets disponibles para el panel Resumen

El panel de resumen incluye widgets que reflejan el panorama actual 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:

Estándares de seguridad

Muestra su puntuación de seguridad resumida más reciente y la puntuación de seguridad de cada estándar 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 de la columna Resultados totales, Security Hub abre una página en la que se muestran los resultados 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 resultados, agrupados por gravedad, en cada Región de AWS en la que se haya habilitado Security Hub. 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.

IAM directores con el mayor número de hallazgos

Proporciona una lista de los 10 AWS Identity and Access Management (IAM) usuarios que han generado la mayoría de los hallazgos. Este widget le ayuda a llevar a cabo tareas administrativas y de facturación. Muestra qué usuarios contribuyen más al uso 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 [elementos informativos administrados por Security Hub](#) y el número de resultados que han generado. Dichos elementos identifican un área de seguridad específica que requiere atención.

Últimos hallazgos de las AWS integraciones

Muestra el número de resultados que ha recibido en Security Hub desde [Servicios de AWS integrados](#). También muestra cuándo recibió por última vez los resultados de cada servicio integrado. Este widget proporciona datos de hallazgos consolidados de múltiples Servicios de AWS. Para obtener más detalles, seleccione un servicio integrado. A continuación, Security Hub abre la consola de ese servicio.

Filtrado del panel Resumen

Puede seleccionar el panel de resumen de la consola de AWS Security Hub 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 del recurso de Amazon de la aplicación (ARN)
- 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)
- 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 `Record state` 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: `aplicaciónARN`, nombre de la 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 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 Guardar.

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 aplica los criterios de ese conjunto 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 predeterminada de Security Hub.

Actualización o eliminación de un conjunto de filtros

1. Abra la consola AWS de Security Hub 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 Resumen

Puede personalizar el panel de resumen de la consola AWS de Security Hub de varias formas. 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 aplica los cambios inmediatamente y guarda la nueva configuración. 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 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.

Creación de recursos de Security Hub con CloudFormation

AWS Security Hub se integra con AWS CloudFormation, que es 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 aprovisione y configure esos recursos por usted.

Cuando la utilice AWS CloudFormation, podrá reutilizar la plantilla para configurar los recursos de Security Hub de forma coherente y repetida. Describa sus recursos una vez y, a continuación, aprovisione los mismos recursos una y otra vez en varias Cuentas de AWS regiones.

Security Hub y AWS CloudFormation plantillas

Para aprovisionar y configurar los recursos de Security Hub y los servicios relacionados, debe entender cómo funcionan las [plantillas de AWS CloudFormation](#). Las plantillas son archivos de texto en YAML formato JSON OR. Estas plantillas describen los recursos que desees aprovisionar en tus AWS CloudFormation pilas.

Si no estás familiarizado con JSON y 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 de Security Hub:

- Habilitación de Security Hub
- Designación del administrador delegado de Security Hub para una organización
- Especificación de la forma en que está configurada su organización en Security Hub
- 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 JSON y YAML plantillas de recursos, consulte la [referencia sobre los tipos de AWS Security Hub recursos](#) en la Guía del AWS CloudFormation usuario.

Obtenga más información sobre AWS CloudFormation

Para obtener más información AWS CloudFormation, consulte los siguientes recursos:

- [AWS CloudFormation](#)
- [AWS CloudFormation Guía del usuario](#)
- [Referencia de AWS CloudFormation API](#)
- [AWS CloudFormation Guía del usuario de la interfaz de línea de comandos](#)

Suscribirse a los anuncios de Security Hub con Amazon SNS

En esta sección se proporciona información sobre cómo suscribirse a los anuncios de AWS Security Hub con Amazon Simple Notification Service (AmazonSNS) para recibir notificaciones sobre Security Hub.


Tras suscribirse, recibirá notificaciones sobre los siguientes eventos (tenga en cuenta el `AnnouncementType` correspondiente a cada evento):

- **GENERAL**: notificaciones generales sobre el servicio Security Hub.
- **UPCOMING_STANDARDS_CONTROLS**: próximamente se publicarán controles o estándares 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 está disponible en una nueva Región de AWS.
- **NEW_STANDARDS_CONTROLS**: se han añadido nuevos controles o estándares de Security Hub.
- **UPDATED_STANDARDS_CONTROLS**: se han actualizado controles o estándares existentes de Security Hub.
- **RETIRED_STANDARDS_CONTROLS**: se han retirado controles o estándares existentes de Security Hub.
- **UPDATED_ASFF**— Se han actualizado la sintaxis, los campos o los valores del AWS Security Finding Format (ASFF).
- **NEW_INTEGRATION**— Están disponibles nuevas integraciones con otros AWS servicios o productos de terceros.
- **NEW_FEATURE**: hay disponibles nuevas características de Security Hub.
- **UPDATED_FEATURE**: se han actualizado las funciones existentes de Security Hub.

Las notificaciones están disponibles en todos los formatos compatibles SNS con Amazon. Puede suscribirse a los anuncios de Security Hub en todas las [Regiones de AWS en las que Security Hub esté disponible](#).

Un usuario debe tener `Subscribe` permisos para suscribirse a un SNS tema de Amazon. Puedes lograrlo con SNS las políticas de Amazon, con IAM las políticas o con ambas. Para obtener más

información, consulta [IAM las SNS políticas de Amazon en conjunto](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

 Note

Security Hub envía SNS anuncios de Amazon sobre las actualizaciones del servicio Security Hub a todos los suscriptores Cuenta de AWS. Para recibir notificaciones sobre los resultados de Security Hub, consulte [Revisión de los detalles de resultados y el historial de resultados en Security Hub](#).

Puedes suscribirte a una cola de Amazon Simple Queue Service (AmazonSQS) para un SNS tema de Amazon, pero debes usar un tema de Amazon (SNS Amazon Resource NameARN) que esté en la misma región. Para obtener más información, consulta el [Tutorial: Suscripción de una SQS cola de Amazon a un SNS tema de Amazon](#) en la Guía para desarrolladores de Amazon Simple Queue Service.

También puedes usar una AWS Lambda función para invocar eventos cuando recibas 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 SNS tema de Amazon ARNs para cada región es el siguiente.

Región de AWS	SNS Tema de Amazon ARN
Este de EE. UU. (Ohio)	arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements
Este de EE. UU. (Norte de Virginia)	arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements
Oeste de EE. UU. (Norte de California)	arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements

Región de AWS	SNSTema de Amazon ARN
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	SNSTema de Amazon ARN
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	SNSTema de Amazon ARN
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>
Oriente Medio (UAE)	<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 (EEUU-Este)	<code>arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements</code>

Región de AWS	SNSTema de Amazon ARN
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 Security Hub.

Para obtener información sobre el coste de la suscripción a los anuncios de Security Hub, consulta los [SNSprecios de Amazon](#).

Suscripción a los anuncios de Security Hub (consola)

1. Abre la SNS consola Amazon en la <https://console.aws.amazon.com/sns/versión 3/home>.
2. En la lista de regiones, seleccione la región en la que desea suscribirse a los anuncios 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. Introduce el tema ARN en el cuadro de temas ARN. Por ejemplo, `arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`.
5. En Protocolo, seleccione cómo desea recibir los anuncios 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 eliges el protocolo de correo electrónico, Amazon SNS enviará un mensaje de confirmación de suscripción al correo electrónico que proporcionaste.

Suscripción a los anuncios 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 eliges el protocolo de correo electrónico, Amazon SNS enviará un mensaje de confirmación de suscripción al correo electrónico que proporcionaste.

Formato de SNS mensaje de Amazon

Los siguientes ejemplos muestran anuncios de Amazon en Security Hub 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 Security Hub para controles nuevos (protocolo de correo electrónico)

```
{
  "AnnouncementType": "NEW_STANDARDS_CONTROLS",
  "Title": "[New Controls] 36 new Security Hub 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 to automatically enable new controls, these controls are enabled by default. Availability of controls can vary by Region. "
}
```

Ejemplo: anuncio de Security Hub para nuevos controles (JSON protocolo de correo electrónico)

```

{
  "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 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 SSecurity
Hub 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" :
"HTHgNFRYMetCvisulgLM4CVySvK9qCXFPHQDxY19tuCFQuIrd7Y04m4YFR28XKMgzqrF20YP
+EilipUm2S0TpEEt0TekU5bn74+YmNZfwr4aPFx0vUuQCV0shmH137hjkiLjhCg/t53QQiLFP7MH
+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUs0G8yiJVCBEJhJ1yS
+gkwJdhRk2UQab9RcAmE6C0K3hRwcjDwqTXz5nR6Ywv1ZqZfLI17gYKslt+jsyd/k+7k0qGm0JRDı7qhE7H
+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"
}

```

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 AWS Security Hub](#)
- [Validación de conformidad para AWS Security Hub](#)
- [Resiliencia en AWS Security Hub](#)
- [Seguridad de la infraestructura en AWS Security Hub](#)
- [AWS Security Hub y VPC puntos finales 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, consulte la sección [Privacidad de datos FAQ](#). Para obtener información sobre la protección de datos en Europa, consulte el [modelo de responsabilidad AWS compartida y](#) la entrada del GDPR blog sobre AWS seguridad.

Para proteger los 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:

- Utilice la autenticación multifactorial (MFA) con cada cuenta.
- UseSSL/TLSpara comunicarse con AWS los recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad del usuario 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.
- Utilice servicios de seguridad gestionados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita entre FIPS 140 y 3 módulos criptográficos validados para acceder a AWS través de una interfaz de línea de comandos o unaAPI, utilice un FIPS terminal. Para obtener más información sobre los FIPS puntos finales disponibles, consulte la [Norma federal de procesamiento de información \(\) 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 consolaAPI, AWS CLI, o AWS SDKs. 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, le recomendamos encarecidamente que no incluya información sobre las credenciales URL para validar la solicitud a 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 AWS 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. IAM los administradores controlan quién puede autenticarse (iniciar sesión) y quién está autorizado (tiene permisos) para usar los recursos de Security Hub. IAM es una Servicio de AWS que puede utilizar sin coste adicional.

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [¿Cómo AWS Security Hub funciona con IAM](#)
- [Ejemplos de políticas basadas en identidades para Security Hub](#)
- [Roles vinculados a servicios de Security Hub](#)
- [AWS políticas gestionadas para AWS Security Hub](#)
- [Solucionar problemas de identidad y acceso de Security Hub](#)

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 [Solucionar problemas de identidad y acceso de Security Hub](#).

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. A continuación, debe enviar solicitudes a su administrador 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 Security Hub, consulte [¿Cómo AWS Security Hub funciona con IAM.](#)

IAM administrador: si es IAM administrador, puede que desee obtener información sobre cómo escribir políticas para administrar el acceso a Security Hub. Para ver ejemplos de políticas basadas en la identidad de Security Hub que puede utilizar IAM, consulte [Ejemplos de políticas basadas en identidades para 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 IAM usuario o asumiendo un IAM rol.

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 (IAM Identity Center), 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 identidad federada, su administrador 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 incluye 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 cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte la [versión 4 de la AWS firma para ver API las solicitudes](#) en la Guía del IAM usuario.

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 multifactorial (MFA) para aumentar la seguridad de su cuenta. Para obtener más información,

consulte [Autenticación multifactorial](#) en la Guía del AWS IAM Identity Center usuario y [Autenticación AWS multifactorial IAM en](#) la Guía del IAM usuario.

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 obtener la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, 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 IAM Identity Center, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus aplicaciones Cuentas de AWS . Para obtener información sobre IAM Identity Center, consulte [¿Qué es IAM Identity Center?](#) en la Guía AWS IAM Identity Center del usuario.

Usuarios y grupos de IAM

Un [IAMusuario](#) es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos utilizar credenciales temporales en lugar de crear IAM usuarios con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales a largo plazo con IAM los usuarios, le recomendamos que rote las claves de acceso. Para obtener 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 puede iniciar sesión como grupo. Puede 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 IAM los recursos.

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 IAM usuarios](#) en la Guía del IAM usuario.

Roles de IAM

Un [IAMrol](#) es una identidad dentro de tu Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Para asumir temporalmente un IAM rol en el AWS Management Console, puede [cambiar de un IAM rol de usuario a uno \(consola\)](#). Puede asumir un rol llamando a una AWS API operación AWS CLI o utilizando una operación personalizadaURL. Para obtener más información sobre los métodos de uso de roles, consulte [Métodos para asumir un rol](#) en la Guía del IAM usuario.

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 los permisos para este. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información sobre las funciones de la federación, consulte [Crear una función para un proveedor de identidades externo \(federación\)](#) en la Guía del IAM usuario. Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM. Para obtener información acerca de los conjuntos de permisos, consulta [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center .
- Permisos IAM de usuario temporales: un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta obtenga acceso a los recursos de su cuenta. Los roles son la forma

principal de conceder acceso entre cuentas. Sin embargo, con algunos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso multicuenta, consulta el tema sobre el acceso a los [recursos entre cuentas IAM en](#) la Guía del IAM usuario.

- **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 IAM usuario o un rol para realizar acciones en AWS ellas, se te considera director. Al utilizar algunos servicios, es posible que realice una acción que, a continuación, inicie otra acción en un servicio diferente. FAS utiliza los permisos de la persona principal que llama a un Servicio de AWS, junto con los que solicitan, Servicio de AWS para realizar solicitudes a los servicios descendentes. FAS las solicitudes 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 detallada sobre la política a la hora de realizar FAS solicitudes, consulte [Reenviar las sesiones de acceso](#).
- **Función de servicio:** una función de servicio es una [IAM función](#) que un servicio asume 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 [Crear un rol para delegar permisos a un Servicio de AWS](#) en la Guía del IAM usuario.
- **Función vinculada a un 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 IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y que realizan AWS CLI o AWS API solicitan. Es preferible hacerlo de este modo a almacenar claves de acceso dentro de la instancia EC2. 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 a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulta [Usar un IAM rol para conceder](#)

[permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon](#) en la Guía del IAM usuario.

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 JSON documentos. Para obtener más información sobre la estructura y el contenido de los documentos de JSON políticas, consulte [Descripción general de JSON las políticas](#) en la Guía del IAM usuario.

Los administradores pueden usar AWS JSON las políticas 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 agregar las políticas de IAM a los roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción, independientemente del método que se utilice 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 AWS Management Console AWS CLI, el o el AWS API.

Políticas basadas en identidad

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, 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 información sobre cómo crear una política basada en la identidad, consulte [Definir IAM permisos personalizados con políticas administradas por el cliente](#) en la Guía del usuario. IAM

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas gestionadas. 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 funciones de su empresa. Cuenta de AWS Las políticas administradas incluyen políticas

AWS administradas y políticas administradas por el cliente. Para saber cómo elegir entre una política gestionada o una política integrada, consulte [Elegir entre políticas gestionadas y políticas integradas en la Guía del IAM](#) usuario.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de buckets de Amazon S3. En los servicios que admiten políticas basadas en recursos, los gestores 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 puede usar políticas AWS administradas desde una política IAM 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 JSON políticas.

Amazon S3 AWS WAF y Amazon VPC son ejemplos de servicios compatibles 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 función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (IAM usuario o rol). Puede 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 JSON políticas 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. 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 JSON políticas que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las IAM políticas asociadas a cada recurso que poseas. Este RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades Usuario raíz de la cuenta de AWS, incluidos los permisos, 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 puede proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener 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 IAM usuario.

¿Cómo AWS Security Hub funciona con IAM

Antes de usar AWS Identity and Access Management (IAM) para administrar el acceso AWS Security Hub, infórmese sobre las IAM funciones disponibles para su uso con Security Hub.

IAM funciones que puede usar 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 las 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 otros dispositivos con la mayoría de IAM las funciones, consulta Servicios de AWS cómo [funcionan IAM](#) en la Guía del IAM usuario.

Políticas basadas en identidad para Security Hub

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, 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 información sobre cómo crear una política basada en la identidad, consulte [Definir IAM permisos personalizados con políticas administradas por el cliente](#) en la Guía del usuario. IAM

Con las políticas basadas en identidades de IAM, puede especificar las acciones permitidas o denegadas, así como los recursos y 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 todos los elementos que puede usar en una JSON política, consulte la [referencia sobre los elementos de la IAM JSON política](#) en la Guía del IAM usuario.

Security Hub es compatible con las políticas basadas en identidad. Para obtener más información, consulte [Ejemplos de políticas basadas en identidades para Security Hub](#).

Políticas basadas en recursos para Security Hub

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos JSON de política que se adjuntan a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de buckets de Amazon S3. En los servicios que admiten políticas basadas en recursos, los gestores 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 hacer posible el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como entidad principal de la política basada en 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 IAM administrador de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) el 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 [Acceso a recursos entre cuentas IAM en](#) la Guía del IAM usuario.

Security Hub no admite políticas basadas en recursos. No puedes adjuntar una IAM política 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 AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El `Action` elemento de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de política suelen tener el mismo nombre que la AWS API operación asociada. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API 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 al `EnableSecurityHub` funcionamiento del Security HubAPI, incluya la `securityhub:EnableSecurityHub` acción 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 para Security Hub](#).

Recursos

Compatibilidad con recursos de políticas: no

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` JSON de política especifica el objeto o los objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso mediante su [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 ARN sintaxis de cada uno de ellos, consulte [Tipos de recursos definidos AWS Security Hub](#) en la Referencia de autorización 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 para 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 AWS JSON políticas 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, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para obtener más información, consulte [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 IAM usuario.

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 para Security Hub](#).

Listas de control de acceso (ACLs) en Security Hub

SoportaACLs: 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 JSON de políticas.

Security Hub no es compatible con ACLs, lo que significa que no puede adjuntar un recurso ACL a un Security Hub.

Control de acceso basado en atributos (ABAC) con Security Hub

Soportes ABAC (etiquetas en las políticas): Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define los permisos en función de los atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a IAM entidades (usuarios o roles) y a muchos AWS recursos. Etiquetar entidades y recursos es el primer paso de ABAC. Luego, diseñe políticas ABAC para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso al que está intentando acceder.

ABAC es útil en entornos de rápido crecimiento y ayuda en situaciones en las que la administración de políticas se vuelve 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 [Definir permisos con ABAC autorización](#) en la Guía del IAM usuario. Para ver un tutorial con los pasos de configuración de ABAC, consulte [Usar el control de acceso basado en atributos \(ABAC\)](#) en la Guía del IAM usuario.

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 recursos de Security Hub](#). 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 para 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 la sección [Servicios de AWS Cómo trabajar con credenciales temporales IAM](#) en la Guía del IAM usuario.

Está utilizando credenciales temporales si inicia sesión AWS Management Console con 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 rol, consulte [Cambiar de un rol de usuario a un IAM rol \(consola\)](#) en la Guía del IAM usuario.

Puede crear credenciales temporales manualmente con la tecla AWS CLI o AWS API. 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 AWS STS API operaciones 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 IAM usuario o un rol para realizar acciones en AWS, se te considera director. Al utilizar algunos servicios, es posible que realice una acción que, a continuación, inicie otra acción

en un servicio diferente. FAS utiliza los permisos de la persona principal que llama a un Servicio de AWS, junto con los que solicitan, Servicio de AWS para realizar solicitudes a los servicios descendentes. FAS las solicitudes 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 detallada sobre la política a la hora de realizar FAS solicitudes, consulte [Reenviar las sesiones de acceso](#).

Por ejemplo, Security Hub realiza FAS solicitudes 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 [Roles vinculados a servicios de 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 [Roles vinculados a servicios de 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 su 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 [Roles vinculados a servicios de Security Hub](#).

Ejemplos de políticas basadas en identidades para 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 con AWS Management Console, AWS CLI, o AWS API. El administrador debe crear IAM políticas que concedan a los usuarios y roles permisos para realizar API operaciones específicas en los recursos específicos que necesitan. El administrador debe asociar esas políticas a los usuarios o grupos que necesiten esos permisos.

Para obtener información sobre cómo crear una política IAM basada en la identidad utilizando estos documentos de JSON política de ejemplo, consulte [Creación de políticas en la JSON pestaña de la Guía del IAM usuario](#).

Temas

- [Prácticas recomendadas sobre las 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 sobre las 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 para 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, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de trabajo](#) 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

puedes llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte [Políticas y permisos en IAM](#) en la Guía de usuario de IAM.

- Use 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 política para especificar que todas las solicitudes deben enviarse mediante 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, consulte [los elementos IAM JSON de la política: Condición](#) en la Guía del IAM usuario.
- Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAM Access Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarlo a crear políticas seguras y funcionales. Para obtener más información, consulte [Validar políticas con IAM Access Analyzer](#) en la Guía del IAM usuario.
- Requerir autenticación multifactorial (MFA): si se encuentra en una situación en la que se requieren IAM usuarios o un usuario raíz Cuenta de AWS, actívela MFA para aumentar la seguridad. Para solicitarlo MFA cuando se convoque a API las operaciones, añada MFA condiciones a sus políticas. Para obtener más información, consulte [API Acceso seguro con MFA](#) en la Guía del IAM usuario.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las [Prácticas recomendadas de seguridad en IAM](#) en la Guía de 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 que tiene en su cuenta 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 realicen llamadas al AWS CLI o al AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la API operación que están intentando 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 [Añadir permisos a un usuario](#) en la Guía del IAM usuario:

```
{
  "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 administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para realizar esta acción en la consola o mediante programación mediante la AWS CLI tecla o. AWS API

```
{
  "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 se puede crear una IAM política 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 esta IAM política funcione, el usuario debe ser el administrador delegado de Security Hub de una 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 se puede crear una IAM política que permita a un usuario ver las conclusiones 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 se puede crear una IAM política que permita a un usuario crear, ver, actualizar y eliminar reglas de automatización de Security Hub. Para que esta IAM política funcione, 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": "*"
    }
  ]
}
```

Roles vinculados a servicios de Security Hub

AWS Security Hub usa un rol vinculado al [servicio AWS Identity and Access Management \(IAM\) denominado `AWSServiceRoleForSecurityHub`](#). Esta función vinculada a un servicio es una IAM función que está vinculada 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 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 sobre otros servicios que admiten funciones vinculadas a servicios, consulte los [AWS servicios con los que funcionan IAM](#) en la Guía del IAM usuario y localice los servicios con la opción Sí en la columna Función vinculada al servicio. 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 a los recursos. AWS Security Hub La función vinculada al servicio permite a Security Hub recibir las conclusiones de otros 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 que una IAM identidad (como un rol, un grupo o un usuario) cree, edite o elimine un rol vinculado a un servicio. Para que el rol `AWSServiceRoleForSecurityHub` vinculado al servicio se cree correctamente, la IAM identidad que utilice 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 `AWSServiceRoleForSecurityHub` vinculado al servicio manualmente mediante la IAM consola, el o el IAMCLI. IAM API

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 sobre la creación manual del rol, consulte [Creación de un rol vinculado a un servicio](#) en la Guía del usuario. 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 utilizando IAM. Para obtener más información, consulte [Edición de un rol vinculado a un servicio](#) en la Guía del usuario. 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 [Deshabilitación de Security Hub](#).

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 la función vinculada al servicio utilizando IAM

Utilice la IAM consola IAMCLI, la o la IAM API para eliminar la función vinculada al `AWSServiceRoleForSecurityHub` servicio. Para obtener más información, consulte [Eliminar un rol vinculado a un servicio](#) en la Guía del usuario. IAM

AWS políticas gestionadas para AWS Security Hub

Una política AWS administrada es una política independiente creada y administrada por AWS. 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 haya nuevas API operaciones disponibles 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 otorga permisos administrativos que brindan a una entidad principal acceso completo a todas las acciones de Security Hub. Esta política debe adjuntarse a una entidad principal antes de que habiliten Security Hub manualmente para sus cuentas. 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`: concede a las entidades principales acceso completo a todas las acciones de Security Hub.
- `guardduty`— Permite a los directores obtener información sobre el estado de las cuentas en Amazon GuardDuty.
- `iam`: permite que las entidades principales creen un rol vinculado a un servicio.
- `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 Servicios de AWS y productos.

```
{
  "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"
            }
        },
        {
            "Sid": "OtherServicePermission",
            "Effect": "Allow",
            "Action": [
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "inspector2:BatchGetAccountStatus",
                "pricing:GetProducts"
            ],
            "Resource": "*"
        }
    ]
}

```

Política gestionada por Security Hub: AWSSecurityHubReadOnlyAccess

Puede adjuntar la política `AWSSecurityHubReadOnlyAccess` a las identidades de IAM.

Esta política otorga permisos de solo lectura que permiten a los usuarios ver información en Security Hub. Las entidades principales con esta política adjunta no pueden realizar ninguna actualización en Security Hub. 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 API las operaciones que comienzan con `GetList`, `oDescribe`.

```

{
    "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 los permisos administrativos necesarios para respaldar la integración de Security Hub con Organizations. AWS Organizations

Estos permisos permiten que la cuenta de administración de la organización designe la cuenta de administrador delegado para Security Hub. También permiten que la cuenta de administrador delegado de Security Hub habilite cuentas de la organización como cuentas miembro.

Esta política solo proporciona los permisos a Organizations. La cuenta de administración de la organización y la cuenta de administrador delegado de Security Hub también requieren permisos para las acciones asociadas en Security Hub. 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 lo 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: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:DescribeOrganization`: permite que las entidades principales recuperen información sobre la configuración de la organización.
- `organizations:EnableAWSServiceAccess`: permite que las entidades principales habiliten la integración de Security Hub con Organizations.
- `organizations:RegisterDelegatedAdministrator`: permite que las entidades principales designen la cuenta de administrador delegado de Security Hub.
- `organizations:DeregisterDelegatedAdministrator`: permite que las entidades principales eliminen la cuenta de administrador delegado de Security Hub.

```
{
  "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:DescribeAccount",

```

```

        "organizations:DescribeOrganizationalUnit"
    ],
    "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"
      }
    }
  }
]
}

```

AWS política gestionada: AWSSecurityHubServiceRolePolicy

No puede adjuntar AWSSecurityHubServiceRolePolicy a sus entidades IAM. Esta política se adjunta a un rol vinculado a un servicio que permite a Security Hub realizar acciones en su nombre. Para obtener más información, consulte [the section called “Roles vinculados a servicios”](#).

Esta política concede permisos administrativos que permiten que el rol vinculado a un servicio ejecute controles de seguridad para los controles de Security Hub.

Detalles de los permisos

Esta política incluye permisos para hacer lo siguiente:

- `cloudtrail`— Recuperar información sobre CloudTrail senderos.
- `cloudwatch`— Recupera las CloudWatch alarmas actuales.
- `logs`— Recupera los filtros métricos para CloudWatch los registros.
- `sns`— Recupera la lista de suscripciones a un SNS tema.
- `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`: recuperar información sobre la configuración del servicio, los estándares y los controles 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"
          ]
        }
      }
    }
  ]
}

```

Security Hub actualiza las políticas AWS gestionadas

Vea los detalles sobre las actualizaciones de las políticas AWS administradas de Security Hub desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbese al RSS feed de la página de [historial de documentos](#) de Security Hub.

Cambio	Descripción	Fecha
AWSSecurityHubFullAccess — Actualización a una política existente	Security Hub 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 actualizó esta política administrada agregando un campo Sid.	22 de febrero de 2024

Cambio	Descripción	Fecha
AWSSecurityHubFullAccess — Actualización a una política existente	Security Hub 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 varias fuentes. Servicios de AWS	16 de noviembre de 2023
AWSSecurityHubOrganizationsAccess — Actualización a una política existente	Security Hub ha actualizado la política para conceder permisos adicionales a fin de permitir acceso de solo lectura a las funcionalidades de administrador delegado de 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 ha agregado los permisos BatchGetSecurityControls , DisassociateFromAdministratorAccount y UpdateSecurityControl para leer y actualizar las propiedades de control de seguridad personalizables.	26 de noviembre de 2023

Cambio	Descripción	Fecha
AWSSecurityHubServiceRolePolicy : actualización de una política actual	Security Hub añadió el permiso <code>tag:GetResources</code> para leer las etiquetas de recursos relacionadas con los resultados.	7 de noviembre de 2023
AWSSecurityHubServiceRolePolicy : actualización de una política actual	Security Hub añadió el permiso <code>BatchGetStandardsControlAssociations</code> 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	Security Hub agregó nuevos permisos para obtener AWS Organizations datos y leer y actualizar las configuraciones del Security Hub, incluidos los estándares y los controles.	20 de septiembre de 2023
AWSSecurityHubServiceRolePolicy : actualización de una política actual	Security Hub trasladó el permiso <code>config:DescribeConfigRuleEvaluationStatus</code> existente a una instrucción diferente en 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 trasladó el permiso <code>config:PutEvaluations</code> existente a una instrucción diferente en 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 añadió un nuevo permiso para permitir que el rol vinculado a un servicio entregue resultados de evaluación a 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 Security Hub.	11 de junio de 2021
AWSSecurityHubOrganizationsAccess — Nueva política	Security Hub añadió una nueva política que otorga los permisos necesarios para la integración de Security Hub con Organizations.	15 de marzo de 2021
Security Hub comenzó a hacer un seguimiento de los cambios	Security Hub comenzó a rastrear los cambios de sus políticas AWS gestionadas.	15 de marzo de 2021

Solucionar problemas de identidad y acceso de Security Hub

Utilice la siguiente información para ayudarle a diagnosticar y solucionar problemas comunes que pueden surgir al trabajar con Security Hub y 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.

El siguiente ejemplo de error se produce cuando un IAM usuario llamado `marymajor` intenta usar 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 AWS el administrador. 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 a AWS.

Para conceder acceso programático a los usuarios, elija una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	Mediante
Identidad del personal (Los usuarios se administran en IAM Identity Center)	Utilice 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: <ul style="list-style-type: none"> • Para el 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 de IAM Identity Center 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 IAM usuario.
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: <ul style="list-style-type: none"> • Para ello AWS CLI, consulte Autenticación con credenciales IAM de usuario 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 de IAM los usuarios en la Guía del IAM usuario.

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 IAM a través de un proveedor de identidad:

Cree un rol para la federación de identidades. Siga las instrucciones de la Guía del IAM usuario sobre cómo [crear un rol para un proveedor de identidades externo \(federación\)](#).

- IAMusuarios:

- Cree un rol que el usuario pueda aceptar. Siga las instrucciones de la Guía del [IAMusuario sobre cómo crear un rol para un](#) IAM usuario.
- (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones de [Añadir permisos a un usuario \(consola\)](#) de la Guía del IAM usuario.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a los recursos de mi Security Hub

Puedes crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puedes 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 AWS Security Hub funciona con IAM](#).
- Para obtener información sobre cómo proporcionar acceso a los recursos de tu Cuentas de AWS propiedad, consulta [Cómo proporcionar acceso a un IAM usuario en otro de tu Cuenta de AWS propiedad en la Guía](#) del IAMusuario.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta [Cómo permitir el acceso a recursos que Cuentas de AWS son propiedad de terceros](#) en la Guía del IAM usuario.

- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte [Proporcionar acceso a usuarios autenticadoPara que su aplicación pueda acceder a s externamente \(federación de identidades\)](#) en la Guía del usuario de IAM.
- Para saber la diferencia entre usar roles y políticas basadas en recursos para el acceso entre cuentas, consulta el tema Acceso a [recursos entre cuentas IAM en](#) la Guía del IAM usuario.

Validación de conformidad para AWS Security Hub

Los auditores externos evalúan la seguridad y el cumplimiento AWS Security Hub como parte de varios programas de AWS cumplimiento. Estos incluyen SOC PCI la Reserva Federal RAMP HIPAA y otros.

Para obtener una lista del alcance Servicios de AWS de los programas de cumplimiento específicos, consulte los [AWS servicios incluidos en el ámbito de aplicación por programa de cumplimiento](#). Para obtener información general, consulte [Programas de conformidad de AWS](#).

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descargar informes en AWS Artifact](#).

Su responsabilidad en el ámbito de la conformidad al usar Security Hub viene determinada por la confidencialidad de los datos, los objetivos de conformidad de su empresa y las leyes y regulaciones aplicables. AWS proporciona los siguientes recursos para ayudarlo con los requisitos de conformidad:

- [Guías de inicio rápido sobre seguridad y cumplimiento](#): estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en la seguridad y el cumplimiento. AWS
- [AWS Recursos de conformidad](#): esta colección de libros de trabajo y guías puede aplicarse a su sector y ubicación.
- [AWS Config](#)— Este AWS servicio evalúa en qué medida las configuraciones de sus recursos cumplen con las prácticas internas, las directrices del sector y las normativas.
- [AWS Security Hub](#)— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar el cumplimiento de los estándares y las mejores prácticas del sector de la seguridad.

Resiliencia en AWS Security Hub

La infraestructura AWS global se basa en Regiones de AWS zonas 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 la 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 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.

APIs llamadas 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). Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Cifre suites con perfecto secreto (PFS), como (Ephemeral Diffie-Hellman) o DHE 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 VPC puntos finales de interfaz ()AWS PrivateLink

Puede establecer una conexión privada entre usted VPC y AWS Security Hub mediante la creación de un VPC punto final de interfaz. Los puntos finales de la interfaz funcionan con una tecnología que le permite acceder de forma privada a Security Hub APIs sin una puerta de enlace a Internet, un NAT dispositivo, una VPN conexión o una conexión AWS Direct Connect. [AWS PrivateLink](#) Las instancias VPC que tenga no necesitan direcciones IP públicas para comunicarse con Security Hub APIs. El tráfico entre tu Security Hub VPC y tú 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 los [VPC puntos finales de la interfaz \(AWS PrivateLink\)](#) en la AWS PrivateLink guía.

Consideraciones sobre los puntos VPC finales de Security Hub

Antes de configurar un VPC punto final de interfaz para Security Hub, asegúrese de revisar las [propiedades y limitaciones del punto final de interfaz](#) en la AWS PrivateLink Guía.

Security Hub permite realizar llamadas a todas sus API acciones desde su VPC.

Note

Security Hub no admite VPC puntos finales en la región de Asia Pacífico (Osaka).

Creación de un VPC punto final de interfaz para Security Hub

Puedes crear un VPC punto final para el servicio Security Hub mediante la VPC consola de Amazon o con AWS Command Line Interface (AWS CLI). Para obtener más información, consulte [Creación de un punto de conexión de interfaz](#) en la Guía de AWS PrivateLink .

Cree un VPC punto final para Security Hub con el siguiente nombre de servicio:

- com.amazonaws. *region*.securityhub

Si habilita la privacidad DNS para el punto final, puede realizar API solicitudes a Security Hub utilizando su DNS nombre predeterminado para la región, por ejemplo `securityhub.us-east-1.amazonaws.com`.

Para obtener más información, consulte [Acceso a un servicio a través de un punto de conexión de interfaz](#) en la Guía de AWS PrivateLink .

Creación de una VPC política de puntos finales para Security Hub

Puede adjuntar una política de punto final a su VPC punto final que controle 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 servicios con VPC puntos finales](#) en la AWS PrivateLink Guía.

Ejemplo: política VPC de puntos finales para las 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 VPC puntos de conexión en las subredes que se comparten con usted. Sin embargo, puede usar los VPC puntos finales en las subredes que compartan con usted. Para obtener información sobre cómo VPC compartir, consulta [Comparte tu cuenta VPC con otras cuentas](#) en la Guía del VPC usuario de Amazon.

Registrar API llamadas de Security Hub con CloudTrail

AWS Security Hub 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. CloudTrail captura API las llamadas a Security Hub como eventos. Las llamadas capturadas incluyen las llamadas desde la consola del Security Hub y las llamadas en código a las API operaciones del Security Hub. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Security Hub. Si no configura un registro, 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, 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 configurarla y habilitarla, consulte la [Guía del AWS CloudTrail usuario](#).

Información sobre Security Hub en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad de eventos admitida en Security Hub, 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 mantener un registro continuo de los eventos de su cuenta, incluidos los eventos de Security Hub, cree un registro de seguimiento. 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 SNS las notificaciones de Amazon para CloudTrail](#)
- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

Security Hub permite registrar todas las API acciones del Security Hub como eventos en CloudTrail los registros. Para ver una lista de las operaciones del Security Hub, consulte la [APIReferencia del Security Hub](#).

Cuando se registra la actividad de las siguientes acciones CloudTrail, el valor de `responseElements` se establece en `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 AWS servicio

Para obtener más información, consulte el [CloudTrail userIdentity elemento](#).

Ejemplo: entradas del archivo de registros 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 usted 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 API llamadas públicas, 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 [Visualizar información en Security Hub](#).

```
{
  "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": "c0fffccd-f04d-11e8-93fc-ddcd14710066",
  "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "012345678901"
}
```

Etiquetado de recursos de Security Hub

Una etiqueta es una etiqueta opcional que puede definir y asignar a AWS los recursos, incluidos ciertos tipos de recursos de AWS Security Hub. 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 agregar etiquetas a los siguientes tipos de recursos 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 la etiqueta asociada 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 AWS de Security Hub, 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 a UTF 8 caracteres. El valor de una etiqueta puede tener un máximo de 256 a UTF 8 caracteres. Los caracteres pueden ser letras, números, espacios o los siguientes símbolos: `_ . : / = + - @`
- El `aws :` prefijo está reservado para su uso por parte AWS de. 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, las etiquetas se aplican solo al recurso que está almacenado directamente en Security Hub en la Región de AWS correspondiente. No se aplican a ningún recurso de apoyo asociado que Security Hub 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 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 sus recursos 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 de ellas, entre ellas. AWS Billing and Cost Management No se diseñaron para utilizarse con datos confidenciales.

Para agregar y administrar etiquetas para los recursos del Security Hub, puede usar la consola Security Hub, el Security Hub API o el AWS Resource Groups EtiquetadoAPI. Con Security Hub, puede agregar etiquetas a un recurso en el momento de su creación. 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.

Para obtener consejos y prácticas recomendadas adicionales sobre el etiquetado, consulte [Cómo etiquetar AWS los recursos en la Guía del usuario sobre cómo etiquetar AWS los recursos](#).

Uso de etiquetas en políticas de IAM

Después de empezar a etiquetar los recursos, puede definir los permisos a nivel de recursos basados en etiquetas en las políticas (). AWS Identity and Access Management IAM Al usar las etiquetas de esta manera, puede implementar un control pormenorizado de los usuarios y roles de su empresa que Cuenta de AWS tienen permiso para crear y etiquetar recursos, y de los usuarios y roles que tienen permiso para añadir, editar y eliminar etiquetas de manera más general. Para controlar el acceso en función de las etiquetas, puede utilizar [claves de condición relacionadas con las etiquetas](#) en el [elemento Condición](#) de IAM las políticas.

Por ejemplo, puede crear una IAM política que permita a un usuario tener acceso completo a todos los recursos de AWS Security Hub, 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 IAM usuario.

Adición de etiquetas a los recursos 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. Con las etiquetas, puede identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Por ejemplo, puede utilizar 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 agregar etiquetas a los siguientes tipos de recursos 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 de Security Hub, puede utilizar la consola de Security Hub o el Security HubAPI. 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 de Security Hub al mismo tiempo, utilice las operaciones de etiquetado del [AWS Resource Groups API](#) [Etiquetado](#).

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 (IAM) que puedan utilizar etiquetas para controlar el acceso a los recursos.

Console

Para agregar etiquetas a un recurso de Security Hub (consola)

Al crear una regla de automatización o una política de configuración, la consola de Security Hub ofrece opciones para agregarle etiquetas. Puede proporcionar la clave y el valor de la etiqueta en la sección Etiquetas.

Security Hub API

Para añadir etiquetas a un recurso de Security Hub (API)

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 el comando [CreateConfigurationPolicy](#)APIo, si lo está utilizando AWS CLI, ejecute el [create-configuration-policy](#)comando.
- Para crear una regla de automatización y añadirle una o más etiquetas, invoque el comando [CreateAutomationRule](#)APIo, si lo está utilizando AWS CLI, ejecute el [create-automation-rule](#)comando.
- Para habilitar Security Hub y añadir una o más etiquetas a su Hub recurso, invoque el comando [EnableSecurityHub](#)APIo, si está utilizando el comando AWS Command Line Interface (AWS CLI), ejecute el [enable-security-hub](#)comando.

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 del Security Hub API o, si utiliza el AWS CLI, ejecute el comando [tag-resource](#). En la solicitud, especifique el nombre del 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 añade 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 CLI comando:

```
$ 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 la política ARN de configuración a la que se va a añadir 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 una operación de etiquetado se realiza correctamente, Security Hub devuelve una respuesta HTTP 200 vacía. De lo contrario, Security Hub devuelve una respuesta de HTTP 4xx ó 500 que indica el motivo del error de la operación.

Edición de etiquetas de recursos 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 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 utilizar 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 agregar etiquetas a los siguientes tipos de recursos 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 del Security Hub, puede usar el Security HubAPI. Actualmente, la consola de Security Hub 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 (IAM) que puedan usar etiquetas para controlar el acceso a los recursos.

Security Hub API

Para editar las etiquetas de un recurso de Security Hub (API)

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 únicamente el valor de etiqueta asociado a una clave de etiqueta, sobrescriba el valor existente mediante la [TagResource](#) operación del Security HubAPI. Si utiliza la AWS CLI, ejecute el comando [tag-resource](#). En tu solicitud, especifica el nombre del recurso de Amazon (ARN) del recurso cuyo valor de etiqueta deseas 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 la política ARN 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 devuelve una respuesta HTTP 200 vacía. De lo contrario, Security Hub devuelve una respuesta de HTTP 4 xx ó 500 que indica el motivo del error de la operación.

Revisión de etiquetas de recursos de Security Hub

Después de añadir o editar etiquetas para los recursos de AWS Security Hub, 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 utilizar 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 agregar etiquetas a los siguientes tipos de recursos 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 Security Hub mediante la consola de Security Hub o el Security HubAPI. 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 de Security Hub al mismo tiempo, utilice las operaciones de etiquetado del [AWS Resource Groups API Etiquetado](#).

Console

Para revisar las etiquetas de un recurso de Security Hub (consola)

1. Con las credenciales del administrador del Security Hub, abra la consola del AWS Security Hub 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 API

Para revisar las etiquetas de un recurso de Security Hub (API)

Para recuperar y revisar las etiquetas de un recurso existente, invoque la [ListTagsForResource](#) API. En la solicitud, utilice el `resourceArn` parámetro para especificar el nombre del recurso de Amazon (ARN) del recurso.

Si está utilizando el AWS CLI, ejecute el [list-tags-for-resource](#) comando y utilice el `resource-arn` parámetro para especificar ARN el 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 completa correctamente, Security Hub devuelve una matriz de 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 de Security Hub que tienen etiquetas y todas las etiquetas asignadas a cada uno de esos recursos, utilice la [GetResources](#) operación de AWS Resource Groups etiquetadoAPI. 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 por cada recurso de Security Hub que tenga etiquetas. Cada objeto especifica el recurso ARN de Security Hub y las claves y valores de etiqueta que se asignan al recurso.

Eliminación de etiquetas de recursos de Security Hub

Si agrega etiquetas a un recurso AWS de Security Hub, puede eliminar una o más de ellas posteriormente. Puede definir etiquetas y asignarlas a recursos de AWS , incluidos ciertos tipos de recursos de Security Hub. Puede agregar, editar y eliminar etiquetas de los siguientes tipos de recursos de Security Hub: reglas de automatización, políticas de configuración y recursos de Hub.

Para eliminar etiquetas de un recurso AWS de Security Hub individual, puede utilizar el Security HubAPI. Actualmente, la consola de Security Hub no admite la eliminación de etiquetas.

Para eliminar etiquetas de varios recursos de Security Hub al mismo tiempo, utilice las operaciones de etiquetado del [AWS Resource Groups APIEtiquetado](#).

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 (IAM) que puedan usar la etiqueta para controlar el acceso a los recursos.

Security Hub API

Para eliminar etiquetas de un recurso de Security Hub (API)

Para eliminar una o más etiquetas de un recurso mediante programación, utilice la [UntagResource](#) operación del Security Hub. API En tu solicitud, usa el `resourceArn` parámetro para especificar el nombre del recurso de Amazon (ARN) del recurso del que quieres 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 utilizas el AWS CLI, ejecuta el comando [untag-resource](#) para eliminar una o más etiquetas de un recurso. Para el `resource-arn` parámetro, especifique el recurso ARN 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 la política ARN de configuración de la que se va a eliminar una etiqueta y `Environment` es la clave 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 devuelve una respuesta HTTP 200 vacía. De lo contrario, Security Hub devuelve una respuesta de HTTP 4 xx ó 500 que indica el motivo del error de la operación.

Cuotas de Security Hub

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 para 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 Security Hub, consulte [Puntos de conexión y cuotas de AWS Security Hub](#) en la Referencia general de AWS.

Cuotas de tarifas

Para obtener una lista de las cuotas que se aplican a las operaciones de la API de Security Hub, consulte [Referencia de la API de AWS Security Hub](#).

Si configura la [agregación entre regiones en Security Hub](#), una llamada a las regiones vinculadas BatchImportFindings y BatchUpdateFindings a la región de agregación afectará a ellas. 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.

Límites regionales de Security Hub

Algunas funciones de AWS Security Hub solo están disponibles en algunas Regiones de AWS. En las siguientes secciones se especifican estos límites regionales.

Para obtener una lista de las regiones en las que está disponible Security Hub, consulte los [puntos de conexión y cuotas de AWS Security Hub](#) en Referencia general de AWS.

Restricciones de agregación entre regiones

En AWS GovCloud (US), [la agregación entre regiones](#) está disponible únicamente para los resultados, las actualizaciones de resultados y los hallazgos contenidos solo en AWS GovCloud (US). En concreto, solo puede agregar resultados, actualizaciones y hallazgos entre AWS GovCloud (EE. UU. Este) y AWS GovCloud (Oeste).

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 obtener una lista de regiones que están deshabilitadas de forma predeterminada, consulte [Habilitar una región](#) en la Referencia general de AWS.

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 de Security Hub al elegir esa región.

Integraciones que son compatibles en China (Pekín) y China (Ningxia)

Las regiones de China (Pekín) y China (Ningxia) solo admiten las siguientes [integraciones de servicios de AWS](#):

- 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 Patch Manager

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 AWS GovCloud (Este de EE. UU.) y AWS GovCloud (Oeste de EE. UU.)

[Las regiones de AWS GovCloud \(Este de EE. UU.\) y AWS GovCloud \(Oeste de EE. UU.\) solo admiten las siguientes integraciones de servicios de 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 (Este de EE. UU.) y AWS GovCloud (Oeste de EE. UU.) 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 AWS GovCloud (Oeste de EE. UU.))
- 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

Estándar gestionado por el servicio: AWS Control Tower solo está disponible en las regiones que admiten AWS Control Tower, como AWS GovCloud (US). Para ver una lista de las regiones AWS Control Tower compatibles, consulte [Cómo funcionan las Regiones de AWS con AWS Control Tower](#) en la Guía del usuario de AWS Control Tower.

El estándar de etiquetado de recursos de AWS no está disponible en el oeste de Canadá (Calgary), en China ni en AWS GovCloud (US).

Hay otros estándares de seguridad disponibles en todas las regiones en las que está disponible Security Hub.

Disponibilidad de los controles por región

Es posible que los controles de Security Hub no estén disponibles en todas las regiones. Para ver una lista de los controles no disponibles en cada región, consulte [Límites regionales para los controles de Security Hub](#). Un control no aparece en la lista de controles de la consola de Security Hub si no está disponible en la región en la que ha iniciado sesión. La excepción se produce si ha iniciado sesión en una región de agregación. En ese caso, puede ver los controles que están disponibles en la región de agregación o en una o más regiones vinculadas.

Límites regionales para los controles de Security Hub

La mayoría AWS de los controles de Security Hub están disponibles solo en una selección Regiones de AWS. Esta página muestra los controles que no están disponibles en cada región. Un control no aparece en la lista de controles de la consola de Security Hub si no está disponible en la región en la que ha iniciado sesión. La excepción se produce si ha iniciado sesión en una región de agregación.

En ese caso, puede ver los controles que están disponibles en la región de agregación o en una o más regiones vinculadas.

Contenido

- [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 \(Yakarta\)](#)
- [Asia-Pacífico \(Hyderabad\)](#)
- [Asia-Pacífico \(Malasia\)](#)
- [Asia-Pacífico \(Melbourne\)](#)
- [Asia-Pacífico \(Bombay\)](#)
- [Asia-Pacífico \(Osaka\)](#)
- [Asia-Pacífico \(Seúl\)](#)
- [Asia-Pacífico \(Singapur\)](#)
- [Asia-Pacífico \(Sídney\)](#)
- [Asia-Pacífico \(Tokio\)](#)
- [Canadá \(centro\)](#)
- [China \(Pekín\)](#)
- [China \(Ningxia\)](#)
- [Europa \(Fráncfort\)](#)
- [Europa \(Irlanda\)](#)
- [Europa \(Londres\)](#)
- [Europa \(Milán\)](#)
- [Europa \(París\)](#)
- [Europa \(España\)](#)
- [Europa \(Estocolmo\)](#)

- [Europa \(Zúrich\)](#)
- [Israel \(Tel Aviv\)](#)
- [Medio Oriente \(Baréin\)](#)
- [Oriente Medio \(UAE\)](#)
- [América del Sur \(São Paulo\)](#)
- [AWS GovCloud \(EEUU-Este\)](#)
- [AWS GovCloud \(EEUU-Oeste\)](#)

Este de EE. UU. (Norte de Virginia)

Los siguientes controles no se admiten en el Este de EE. UU. (Norte de Virginia).

- [\[ElastiCache.4\] 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 \(RedisOSS\) de versiones anteriores deberían tener Redis activado OSS AUTH](#)
- [\[ElastiCache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[S3.24\] 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 el Este de EE. UU. (Ohio).

- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)

- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[EC2.24\] No se deben usar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.26\] 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](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)
- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

Oeste de EE. UU. (Norte de California)

Los siguientes controles no se admiten en el Oeste de EE. UU. (Norte de California).

- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)

- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[DocumentDB.1\] 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](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.26\] 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 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](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)
- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

Oeste de EE. UU. (Oregón)

Los siguientes controles no se admiten en el Oeste de EE. UU. (Oregón).

- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[ECR.4\] Los repositorios ECR públicos 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](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web 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 África (Ciudad del Cabo).

- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[CodeBuild.1\] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales](#)
- [\[Cognito.1\] 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](#)
- [\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)
- [\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización 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](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.3\] Los volúmenes adjuntos de Amazon EBS deben cifrarse en reposo](#)
- [\[EC2.4\] 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](#)
- [\[EC2.12\] Amazon no utilizado EC2 EIPs debería retirarse](#)
- [\[EC2.13\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o :/0 al puerto 22](#)
- [\[EC2.14\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o :/0 al puerto 3389](#)

- [\[EC2.24\] No se deben usar 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](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] EFS Los volúmenes de Amazon deberían estar en los planes de respaldo](#)
- [\[ELB.1\] Application Load Balancer debe configurarse para redirigir todas las HTTP solicitudes a HTTPS](#)
- [\[ELB.2\] Los balanceadores de carga clásicos con HTTPS listenersSSL/deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.4\] Application Load Balancer debe configurarse para eliminar los encabezados http no válidos](#)
- [\[ELB.8\] Los balanceadores de carga clásicos que utilizan dispositivos de SSL escucha deben usar una política de seguridad predefinida que tenga una larga duración AWS Config](#)
- [\[ELB.16\] Los balanceadores de carga de aplicaciones deben estar asociados a una web AWS WAF ACL](#)
- [\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)
- [\[ES.3\] 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](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.18\] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[IoT.1\] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse](#)
- [\[IoT.2\] Las acciones de mitigación de AWS IoT Core deben etiquetarse](#)
- [\[IoT.3\] Las dimensiones de AWS IoT Core deben etiquetarse](#)
- [\[IoT.4\] Los autorizadores de AWS IoT Core deben etiquetarse](#)
- [\[IoT.5\] Los alias de los roles de AWS IoT Core deben etiquetarse](#)

- [\[IoT.6\] Las políticas de AWS IoT Core deben etiquetarse](#)
- [\[MSK.3\] Los conectores MSK Connect deben estar cifrados en tránsito](#)
- [\[RDS.1\] La instantánea de RDS debe ser privada](#)
- [\[RDS.9\] 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](#)
- [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 clústeres de Amazon Redshift \[Redshift.3\] deben tener habilitadas las instantáneas automáticas](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas 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 AI notebook no deberían tener acceso directo a Internet](#)
- [\[SSM.2\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche](#)
- [\[SSM.3\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado](#)

Asia-Pacífico (Hong Kong)

Los siguientes controles no se admiten en Asia-Pacífico (Hong Kong).

- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)

- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[Cognito.1\] 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](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.24\] No se deben usar 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](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)

- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[MSK.3\] Los conectores MSK Connect deben estar cifrados en tránsito](#)
- [La autenticación de IAM \[RDS.10\] debe configurarse para las instancias de RDS](#)
- [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](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas 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](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)
- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

Asia-Pacífico (Yakarta)

Los siguientes controles no se admiten en Asia-Pacífico (Yakarta).

- [\[Account.2\] Cuentas de AWS debe ser parte de una organización de AWS Organizations](#)
- [\[APIGateway.1\] La API puerta de enlace REST y el registro de WebSocket API ejecuciones deben estar habilitados](#)
- [\[APIGateway.2\] REST API Las etapas de la API puerta de enlace deben configurarse para usar SSL certificados para la autenticación de fondo](#)
- [\[APIGateway.3\] REST API Las etapas de API Gateway deben tener habilitado el AWS X-Ray rastreo](#)
- [\[APIGateway.4\] La API puerta de enlace debe estar asociada a una web WAF ACL](#)
- [\[APIGateway.8\] Las rutas de API gateway deben especificar un tipo de autorización](#)

- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas de API Gateway V2](#)
- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[AutoScaling.5\] EC2 Las instancias de Amazon lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas](#)
- [Los puntos de recuperación de \[Backup.1\] AWS Backup deben estar cifrados en reposo](#)
- [\[Backup.2\] Los puntos de recuperación de AWS Backup deben etiquetarse](#)
- [\[Backup.4\] Los planes de informes de AWS Backup deben etiquetarse](#)
- [\[CloudFormation.2\] Las pilas de CloudFormation deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[CodeBuild.1\] 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](#)
- [\[Cognito.1\] 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](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)
- [\[DMS.2\] DMS los certificados deben estar etiquetados](#)
- [\[DMS.3\] las suscripciones a DMS eventos deben estar etiquetadas](#)
- [\[DMS.4\] las instancias de DMS replicación deben estar etiquetadas](#)
- [\[DMS.5\] los grupos de subredes de DMS replicación deben estar etiquetados](#)
- [\[DMS.6\] las instancias de DMS replicación deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] las tareas de DMS replicación de la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] las tareas de DMS replicación de la base de datos de origen deben tener el registro activado](#)
- [\[DMS.9\] Los DMS puntos finales deben utilizar SSL](#)
- [\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización IAM](#)
- [\[DMS.11\] DMS Los puntos finales de MongoDB deberían tener habilitado un mecanismo de autenticación](#)
- [\[DMS.12\] DMS Los puntos finales de Redis deberían estar habilitados OSS TLS](#)
- [\[DocumentDB.1\] 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 \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.4\] 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](#)
- [\[EC2.13\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 22](#)
- [\[EC2.14\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 3389](#)
- [\[EC2.18\] Los grupos de seguridad solo deberían permitir el tráfico entrante sin restricciones en los puertos autorizados](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon no utilizados deberían eliminarse](#)
- [\[EC2.24\] No se deben usar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de respaldo](#)
- [\[EC2.51\] Los puntos finales de 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](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[ECS.9\] las definiciones de ECS tareas deben tener una configuración de registro](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] EFS Los volúmenes de Amazon deberían estar en los planes de respaldo](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(RedisOSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(RedisOSS\) de versiones anteriores deberían tener Redis activado OSS AUTH](#)
- [\[ElastiCache.7\] 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](#)
- [\[ES.1\] 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](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[Glue.1\] los AWS Glue trabajos deben estar etiquetados](#)
- [\[Glue.3\] Las transformaciones AWS Glue de aprendizaje automático deben cifrarse en reposo](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[IAM.18\] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[IoT.1\] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse](#)
- [\[IoT.2\] Las acciones de mitigación de AWS IoT Core deben etiquetarse](#)
- [\[IoT.3\] Las dimensiones de AWS IoT Core deben etiquetarse](#)
- [\[IoT.4\] Los autorizadores de AWS IoT Core deben etiquetarse](#)
- [\[IoT.5\] Los alias de los roles de AWS IoT Core deben etiquetarse](#)
- [\[IoT.6\] Las políticas de AWS IoT Core deben etiquetarse](#)
- [\[Macie.1\] Amazon Macie debe estar habilitado](#)
- [\[Macie.2\] La detección automática de datos confidenciales de Macie debe estar habilitada](#)
- [\[MSK.3\] Los conectores MSK Connect deben estar cifrados 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 bases de datos de Neptune deben tener habilitada la autenticación de bases de datos 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](#)
- [\[RDS.9\] Las instancias de base de datos de RDS deben publicar los registros en Logs CloudWatch](#)
- [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](#)
- [\[Redshift.1\] 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](#)
- [\[Redshift.7\] Los clústeres de Redshift deberían utilizar un enrutamiento mejorado VPC](#)
- [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](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas 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](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker AI notebook no deberían tener acceso directo a Internet](#)
- [\[ServiceCatalog.1\] Las carteras de Service Catalog solo deben compartirse dentro de una organización de AWS](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)

- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SSM.1\] EC2 Las instancias de Amazon deben gestionarse mediante AWS Systems Manager](#)
- [\[SSM.2\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche](#)
- [\[SSM.3\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.3\] Los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.10\] la AWS WAF web ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)
- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

Asia-Pacífico (Hyderabad)

Los siguientes controles no se admiten en Asia-Pacífico (Hyderabad).

- [\[Account.2\] Cuentas de AWS debe ser parte de una organización de AWS Organizations](#)
- [\[APIGateway.3\] REST API Las etapas de API Gateway deben tener habilitado el AWS X-Ray rastreo](#)
- [\[APIGateway.4\] La API puerta de enlace debe estar asociada a una web WAF ACL](#)
- [\[APIGateway.8\] Las rutas de API gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas de API Gateway V2](#)
- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[Athena.4\] Los grupos de trabajo de Athena deben tener el registro habilitado](#)
- [Los puntos de recuperación de \[Backup.1\] AWS Backup deben estar cifrados en reposo](#)
- [\[Backup.2\] Los puntos de recuperación de AWS Backup deben etiquetarse](#)
- [\[Backup.4\] Los planes de informes de AWS Backup deben etiquetarse](#)
- [\[CloudFormation.2\] Las pilas de CloudFormation deben etiquetarse](#)

- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CloudTrail.6\] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público](#)
- [\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[CodeBuild.1\] 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](#)
- [\[CodeBuild.7\] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo](#)
- [\[Cognito.1\] 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](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)
- [\[DMS.2\] DMS los certificados deben estar etiquetados](#)

- [\[DMS.3\] las suscripciones a DMS eventos deben estar etiquetadas](#)
- [\[DMS.4\] las instancias de DMS replicación deben estar etiquetadas](#)
- [\[DMS.5\] los grupos de subredes de DMS replicación deben estar etiquetados](#)
- [\[DMS.6\] las instancias de DMS replicación deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] las tareas de DMS replicación de la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] las tareas de DMS replicación de la base de datos de origen deben tener el registro activado](#)
- [\[DMS.9\] Los DMS puntos finales deben utilizar SSL](#)
- [\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización IAM](#)
- [\[DMS.11\] DMS Los puntos finales de MongoDB deberían tener habilitado un mecanismo de autenticación](#)
- [\[DMS.12\] DMS Los puntos finales de Redis deberían estar habilitados OSS TLS](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.4\] 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](#)
- [\[EC2.13\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o :/0 al puerto 22](#)
- [\[EC2.14\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o :/0 al puerto 3389](#)
- [\[EC2.18\] Los grupos de seguridad solo deberían permitir el tráfico entrante sin restricciones en los puertos autorizados](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon no utilizados deberían eliminarse](#)
- [\[EC2.24\] No se deben usar 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 respaldo](#)
- [\[EC2.34\] Las tablas de rutas de las pasarelas de EC2 tránsito deben estar etiquetadas](#)
- [\[EC2.40\] Las pasarelas EC2 NAT deben estar etiquetadas](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben estar etiquetados](#)

- [\[EC2.51\] Los puntos finales de 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 utilizar la versión 2 \(\) del Servicio de Metadatos de Instancia IMDSv2](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[ECS.9\] las definiciones de ECS tareas deben tener una configuración de registro](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] EFS Los volúmenes de Amazon deberían estar en los planes de respaldo](#)
- [\[ELB.5\] El registro de aplicaciones y balanceadores de carga clásicos debe estar habilitado](#)
- [\[ELB.14\] El Classic Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(RedisOSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(RedisOSS\) de versiones anteriores deberían tener Redis activado OSS AUTH](#)
- [\[ElastiCache.7\] 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](#)
- [\[ES.1\] 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](#)

- [\[EventBridge.3\] 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](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[Glue.1\] los AWS Glue trabajos deben estar etiquetados](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[GuardDuty.9\] La GuardDuty RDS protección 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](#)
- [\[IAM.5\] 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](#)
- [\[IAM.18\] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte](#)
- [\[IAM.19\] 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 la política adjunta AWSCloud ShellFullAccess](#)
- [\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.2\] El ECR escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.3\] 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](#)
- [\[IoT.1\] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse](#)
- [\[IoT.2\] Las acciones de mitigación de AWS IoT Core deben etiquetarse](#)

- [\[IoT.3\] Las dimensiones de AWS IoT Core deben etiquetarse](#)
- [\[IoT.4\] Los autorizadores de AWS IoT Core deben etiquetarse](#)
- [\[IoT.5\] Los alias de los roles de AWS IoT Core deben etiquetarse](#)
- [\[IoT.6\] Las políticas de AWS IoT Core deben etiquetarse](#)
- [\[KMS.1\] 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 MSK Connect deben estar cifrados 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 bases de datos de Neptune deben tener habilitada la autenticación de bases de datos 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](#)
- [\[RDS.2\] Las instancias de base de datos de RDS deben prohibir el acceso público, según lo determine la configuración PubliclyAccessible](#)
- [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 \[RDS.12\] debe configurarse para los clústeres de RDS](#)
- [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](#)
- [\[Redshift.1\] 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](#)
- [Amazon Redshift \[Redshift.6\] debería tener habilitadas las actualizaciones automáticas a las versiones principales](#)
- [\[Redshift.7\] Los clústeres de Redshift deberían utilizar un enrutamiento mejorado VPC](#)
- [Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.6\] Las políticas de compartimentos de uso general de S3 deberían restringir el acceso a otros Cuentas de AWS](#)
- [\[S3.17\] Los depósitos de uso general de S3 deben cifrarse en reposo con AWS KMS keys](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker AI notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] Las instancias de SageMaker AI notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker AI Notebook](#)
- [\[SES.1\] 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](#)
- [\[SSM.1\] EC2 Las instancias de Amazon deben gestionarse mediante AWS Systems Manager](#)
- [\[SSM.2\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche](#)
- [\[SSM.3\] EC2 Las instancias de Amazon gestionadas 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](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)

- [\[WAF.3\] Los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.10\] la AWS WAF web ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)
- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

Asia-Pacífico (Malasia)

Los siguientes controles no se admiten en Asia Pacífico (Malasia).

- [\[ACM.1\] Los certificados importados y ACM emitidos deben renovarse después de un período de tiempo específico](#)
- [\[ACM.2\] RSA los certificados gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)
- [\[ACM.3\] ACM los certificados deben estar etiquetados](#)
- [\[Account.1\] La información de contacto de seguridad debe proporcionarse para una Cuenta de AWS](#)
- [\[Account.2\] Cuentas de AWS debe ser parte de una organización de AWS Organizations](#)
- [\[APIGateway.1\] La API puerta de enlace REST y el registro de WebSocket API ejecuciones deben estar habilitados](#)
- [\[APIGateway.2\] REST API Las etapas de la API puerta de enlace deben configurarse para usar SSL certificados para la autenticación de fondo](#)
- [\[APIGateway.3\] REST API Las etapas de API Gateway deben tener habilitado el AWS X-Ray rastreo](#)
- [\[APIGateway.4\] La API puerta de enlace debe estar asociada a una web WAF ACL](#)
- [\[APIGateway.5\] Los datos de la REST API caché 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 de API Gateway V2](#)
- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)

- [\[AppSync.2\] AWS AppSync debe tener activado 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 API](#)
- [\[AppSync.6\] AWS AppSync API Las cachés 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](#)
- [\[AutoScaling.1\] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar controles de ELB estado](#)
- [\[AutoScaling.2\] 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](#)
- [\[AutoScaling.5\] EC2 Las instancias de Amazon lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas](#)
- [Los puntos de recuperación de \[Backup.1\] AWS Backup deben estar cifrados en reposo](#)
- [\[Backup.2\] Los puntos de recuperación de AWS Backup deben etiquetarse](#)
- [\[Backup.3\] Los almacenes de AWS Backup deben etiquetarse](#)
- [\[Backup.4\] Los planes de informes de AWS Backup deben etiquetarse](#)
- [\[Backup.5\] Los planes de copias de seguridad de AWS Backup deben etiquetarse](#)
- [\[CloudFormation.2\] Las pilas de CloudFormation deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)

- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CloudTrail.6\] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público](#)
- [\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3](#)
- [\[CloudWatch.17\] Las acciones de alarma de CloudWatch deben estar activadas](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[CodeBuild.1\] 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](#)
- [\[Cognito.1\] 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](#)
- [\[DataFirehose.1\] Los flujos de entrega de Firehose deben estar cifrados en reposo](#)
- [\[DataSync.1\] Las tareas de DataSync deben tener el registro habilitado](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)
- [\[DMS.2\] DMS los certificados deben estar etiquetados](#)

- [\[DMS.3\] las suscripciones a DMS eventos deben estar etiquetadas](#)
- [\[DMS.4\] las instancias de DMS replicación deben estar etiquetadas](#)
- [\[DMS.5\] los grupos de subredes de DMS replicación deben estar etiquetados](#)
- [\[DMS.6\] las instancias de DMS replicación deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] las tareas de DMS replicación de la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] las tareas de DMS replicación de la base de datos de origen deben tener el registro activado](#)
- [\[DMS.9\] Los DMS puntos finales deben utilizar SSL](#)
- [\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización IAM](#)
- [\[DMS.11\] DMS Los puntos finales de MongoDB deberían tener habilitado un mecanismo de autenticación](#)
- [\[DMS.12\] DMS Los puntos finales de Redis deberían estar habilitados OSS TLS](#)
- [\[DocumentDB.1\] 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 \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.4\] 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](#)
- [\[EC2.4\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.21\] La red no ACLs debe permitir la entrada desde el 0.0.0.0/0 al puerto 22 o al puerto 3389](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon no utilizados deberían eliminarse](#)

- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC2.24\] No se deben usar 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 respaldo](#)
- [\[EC2.33\] Los archivos adjuntos a las pasarelas de EC2 tránsito deben estar etiquetados](#)
- [\[EC2.34\] Las tablas de rutas de las pasarelas de EC2 tránsito deben estar etiquetadas](#)
- [\[EC2.37\] Las direcciones IP EC2 elásticas deben estar etiquetadas](#)
- [\[EC2.40\] Las pasarelas EC2 NAT deben estar etiquetadas](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben estar etiquetados](#)
- [\[EC2.51\] Los puntos finales de EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)
- [\[EC2.52\] Las pasarelas de EC2 tránsito deben estar etiquetadas](#)
- [\[EC2.53\] los grupos de EC2 seguridad no deberían permitir la entrada desde el 0.0.0.0/0 a los puertos de administración remota del servidor](#)
- [\[EC2.54\] Los grupos EC2 de seguridad no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor](#)
- [\[EC2.55\] 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 utilizar la versión 2 \(\) del Servicio de Metadatos de Instancia IMDSv2](#)
- [\[EC2.171\] Las conexiones EC2 VPN deben tener el registro activado](#)
- [\[ECR.1\] Los repositorios ECR privados deben tener configurado el escaneo de imágenes](#)
- [\[ECR.2\] Los repositorios ECR privados deben tener configurada la inmutabilidad de las etiquetas](#)
- [\[ECR.3\] ECR Los repositorios deben tener configurada al menos una política de ciclo de vida](#)

- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[ECS.1\] Las definiciones de ECS tareas de Amazon deben tener modos de red seguros y definiciones de usuario.](#)
- [\[ECS.3\] las definiciones de ECS tareas no deben compartir el espacio de nombres del proceso del host](#)
- [\[ECS.4\] los ECS contenedores deberían ejecutarse sin privilegios](#)
- [\[ECS.5\] ECS Los contenedores 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 ECS tareas deben tener una configuración de registro](#)
- [\[ECS.10\] Los servicios de ECS Fargate deberían ejecutarse en la última versión de la plataforma Fargate](#)
- [\[ECS.12\] ECS los clústeres deben usar Container Insights](#)
- [\[ECS.16\] Los conjuntos de ECS tareas 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](#)
- [\[EFS.2\] EFS Los volúmenes de Amazon deberían estar en los planes de respaldo](#)
- [\[EFS.3\] los puntos de EFS acceso deben establecer un directorio raíz](#)
- [\[EFS.4\] los puntos de EFS acceso deben imponer la identidad de un usuario](#)
- [\[EFS.5\] los puntos de EFS acceso deben estar etiquetados](#)
- [\[EFS.6\] Los destinos de EFS montaje no deben estar asociados a una subred pública](#)
- [\[EFS.7\] los sistemas de EFS archivos deben tener habilitadas las copias de seguridad automáticas](#)
- [\[EFS.8\] los sistemas de EFS archivos deben cifrarse en reposo](#)
- [\[EKS.1\] Los puntos finales de los EKS clústeres no deben ser de acceso público](#)
- [\[EKS.2\] EKS los clústeres deberían ejecutarse en una versión compatible de Kubernetes](#)
- [\[EKS.3\] los EKS clústeres deben usar secretos de Kubernetes cifrados](#)
- [\[EKS.6\] EKS los clústeres deben estar etiquetados](#)
- [\[EKS.7\] Las configuraciones de los proveedores de EKS identidad deben estar etiquetadas](#)
- [\[EKS.8\] EKS los clústeres deben tener habilitado el registro de auditoría](#)
- [\[ELB.2\] Los balanceadores de carga clásicos con HTTPS listenersSSL/deben usar un certificado proporcionado por AWS Certificate Manager](#)

- [\[ELB.10\] Classic Load Balancer debe abarcar varias zonas de disponibilidad](#)
- [\[ELB.12\] Application Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.13\] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad](#)
- [\[ELB.14\] El Classic Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.16\] Los balanceadores de carga de aplicaciones deben estar asociados a una web AWS WAF ACL](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(RedisOSS\) 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 \(RedisOSS\) de versiones anteriores deberían tener Redis activado OSS AUTH](#)
- [\[ElastiCache.7\] 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](#)
- [\[ES.1\] 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](#)

- [\[ES.9\] 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](#)
- [\[FSx.1\] FSx para sistemas de ZFS archivos abiertos, debe configurarse para copiar etiquetas a 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 etiquetarse](#)
- [\[Glue.1\] los AWS Glue trabajos deben estar etiquetados](#)
- [\[Glue.3\] Las transformaciones AWS Glue de aprendizaje automático deben cifrarse en reposo](#)
- [\[GuardDuty.1\] GuardDuty debe 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 del registro de GuardDuty EKS auditoría debe estar habilitada](#)
- [\[GuardDuty.6\] La protección GuardDuty Lambda debe estar habilitada](#)
- [\[GuardDuty.7\] La monitorización del GuardDuty EKS tiempo de ejecución debe estar habilitada](#)
- [\[GuardDuty.8\] La protección contra GuardDuty malware para EC2 debe estar habilitada](#)
- [\[GuardDuty.9\] La GuardDuty RDS protección debe estar habilitada](#)
- [\[GuardDuty.10\] La protección GuardDuty S3 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 para los usuarios de IAM deben tener una duración estricta](#)
[AWS Config](#)
- [\[IAM.11\] 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](#)
- [\[IAM.18\] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte](#)
- [\[IAM.19\] 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 la política adjunta 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 ECR escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.3\] 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](#)
- [\[IoT.1\] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse](#)

- [\[IoT.2\] Las acciones de mitigación de AWS IoT Core deben etiquetarse](#)
- [\[IoT.3\] Las dimensiones de AWS IoT Core deben etiquetarse](#)
- [\[IoT.4\] Los autorizadores de AWS IoT Core deben etiquetarse](#)
- [\[IoT.5\] Los alias de los roles de AWS IoT Core deben etiquetarse](#)
- [\[IoT.6\] Las políticas de AWS IoT Core deben etiquetarse](#)
- [\[Kinesis.1\] 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 VPC Lambda 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](#)
- [\[MSK.1\] MSK Los clústeres deben cifrarse en tránsito entre los nodos intermediarios](#)
- [\[MSK.2\] MSK los clústeres deben tener configurada una supervisión mejorada](#)
- [\[MSK.3\] Los conectores MSK Connect deben estar cifrados 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 bases de datos de Neptune deben tener habilitada la autenticación de bases de datos 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](#)
- [\[NetworkFirewall.1\] Los 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](#)
- [\[NetworkFirewall.7\] Los firewall de Network Firewall se deben etiquetar](#)
- [\[NetworkFirewall.8\] Las políticas de firewall de Network Firewall se deben etiquetar](#)
- [Los firewalls de Network Firewall \[NetworkFirewall.9\] 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](#)
- [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 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 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](#)
- [\[RDS.30\] 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](#)
- [\[RDS.34\] 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](#)
- [\[Redshift.1\] 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](#)
- [\[Redshift.7\] Los clústeres de Redshift deberían utilizar un enrutamiento mejorado VPC](#)
- [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](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas 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](#)
- [\[S3.17\] 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 cubos de uso general de S3 deberían tener habilitada la función de eliminación 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 AI notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] Las instancias de SageMaker AI notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker AI Notebook](#)
- [\[SageMaker.4\] Las variantes de producción de terminales de SageMaker IA deben tener un recuento inicial de instancias superior a 1](#)
- [\[SES.1\] 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](#)
- [\[ServiceCatalog.1\] Las carteras de Service Catalog solo deben compartirse dentro de una organización de AWS](#)
- [\[SNS.4\] las políticas de acceso a los SNS temas 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](#)
- [\[SSM.1\] EC2 Las instancias de Amazon deben gestionarse mediante AWS Systems Manager](#)
- [\[SSM.2\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche](#)

- [\[SSM.3\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [\[SSM.4\] SSM los documentos no deben ser públicos](#)
- [\[StepFunctions.1\] Las máquinas de estado de Step Functions deberían tener el registro activado](#)
- [\[StepFunctions.2\] Las actividades de Step Functions deben estar etiquetadas](#)
- [\[Transfer.1\] AWS Transfer Family Los flujos de trabajo deben estar etiquetados](#)
- [\[Transfer.2\] Los servidores Transfer Family no deben usar el FTP protocolo para la conexión de puntos finales](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.2\] Las reglas regionales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.3\] Los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.4\] La web regional AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.10\] la AWS WAF web ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado](#)
- [\[WAF.12\] AWS WAF las reglas deben tener las CloudWatch métricas habilitadas](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)
- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

Asia-Pacífico (Melbourne)

Los siguientes controles no se admiten en Asia-Pacífico (Melbourne).

- [\[ACM.1\] Los certificados importados y ACM emitidos deben renovarse después de un período de tiempo específico](#)
- [\[APIGateway.8\] Las rutas de API gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas de API Gateway V2](#)
- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.2\] AWS AppSync debe tener activado el registro a nivel de campo](#)

- [\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves API](#)
- [\[AppSync.6\] AWS AppSync API Las cachés 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 controles de ELB estado](#)
- [\[AutoScaling.5\] EC2 Las instancias de Amazon lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas](#)
- [Los puntos de recuperación de \[Backup.1\] AWS Backup deben estar cifrados en reposo](#)
- [\[Backup.2\] Los puntos de recuperación de AWS Backup deben etiquetarse](#)
- [\[Backup.4\] Los planes de informes de AWS Backup deben etiquetarse](#)
- [\[CloudFormation.2\] Las pilas de CloudFormation deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[CodeBuild.1\] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales](#)

- [\[CodeBuild.7\] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo](#)
- [\[Cognito.1\] 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](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)
- [\[DMS.2\] DMS los certificados deben estar etiquetados](#)
- [\[DMS.3\] las suscripciones a DMS eventos deben estar etiquetadas](#)
- [\[DMS.4\] las instancias de DMS replicación deben estar etiquetadas](#)
- [\[DMS.5\] los grupos de subredes de DMS replicación deben estar etiquetados](#)
- [\[DMS.6\] las instancias de DMS replicación deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] las tareas de DMS replicación de la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] las tareas de DMS replicación de la base de datos de origen deben tener el registro activado](#)
- [\[DMS.9\] Los DMS puntos finales deben utilizar SSL](#)
- [\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización IAM](#)
- [\[DMS.11\] DMS Los puntos finales de MongoDB deberían tener habilitado un mecanismo de autenticación](#)
- [\[DMS.12\] DMS Los puntos finales de Redis deberían estar habilitados OSS TLS](#)
- [\[DocumentDB.1\] 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 \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.4\] 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 deberían poder restaurarse públicamente](#)
- [\[EC2.4\] 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](#)
- [\[EC2.9\] EC2 Las instancias de Amazon no deben tener una dirección pública IPv4](#)
- [\[EC2.13\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 22](#)
- [\[EC2.14\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 3389](#)
- [\[EC2.18\] Los grupos de seguridad solo deberían permitir el tráfico entrante sin restricciones en los puertos autorizados](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon no utilizados deberían eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC2.24\] No se deben usar 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 respaldo](#)
- [\[EC2.34\] Las tablas de rutas de las pasarelas de EC2 tránsito deben estar etiquetadas](#)
- [\[EC2.40\] Las pasarelas EC2 NAT deben estar etiquetadas](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben estar etiquetados](#)
- [\[EC2.51\] Los puntos finales de 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 utilizar la versión 2 \(\) del Servicio de Metadatos de Instancia IMDSv2](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)

- [\[ECS.1\] Las definiciones de ECS tareas de Amazon deben tener modos de red seguros y definiciones de usuario.](#)
- [\[ECS.9\] las definiciones de ECS tareas deben tener una configuración de registro](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] EFS Los volúmenes de Amazon deberían estar en los planes de respaldo](#)
- [\[ELB.14\] El Classic Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(RedisOSS\) 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 \(RedisOSS\) de versiones anteriores deberían tener Redis activado OSS AUTH](#)
- [\[ElastiCache.7\] 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](#)
- [\[ES.1\] 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](#)
- [\[EventBridge.3\] 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](#)
- [\[FSx.1\] FSx para sistemas de ZFS archivos abiertos, debe configurarse para copiar etiquetas a copias de seguridad y volúmenes](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[Glue.1\] los AWS Glue trabajos deben estar etiquetados](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[GuardDuty.9\] La GuardDuty RDS protección 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](#)
- [\[IAM.5\] 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 para los usuarios de IAM deben tener una duración estricta AWS Config](#)
- [\[IAM.11\] 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](#)
- [\[IAM.18\] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte](#)
- [\[IAM.19\] 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 la política adjunta AWSCloud ShellFullAccess](#)
- [\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.2\] El ECR escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.3\] 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](#)
- [\[IoT.1\] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse](#)
- [\[IoT.2\] Las acciones de mitigación de AWS IoT Core deben etiquetarse](#)
- [\[IoT.3\] Las dimensiones de AWS IoT Core deben etiquetarse](#)
- [\[IoT.4\] Los autorizadores de AWS IoT Core deben etiquetarse](#)
- [\[IoT.5\] Los alias de los roles de AWS IoT Core deben etiquetarse](#)
- [\[IoT.6\] Las políticas de AWS IoT Core deben etiquetarse](#)
- [\[Kinesis.1\] 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](#)
- [\[MQ.2\] 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](#)
- [\[MSK.3\] Los conectores MSK Connect deben estar cifrados 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 bases de datos de Neptune deben tener habilitada la autenticación de bases de datos 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](#)
- [\[RDS.3\] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo](#)

- [Los clústeres de RDS \[RDS.7\] deben tener habilitada la protección contra la eliminación](#)
- [La autenticación de IAM \[RDS.12\] debe configurarse para los clústeres de RDS](#)
- [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](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.14\] 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](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker AI notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] Las instancias de SageMaker AI notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker AI Notebook](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [\[SNS.1\] SNS los temas deben cifrarse en reposo mediante AWS KMS](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SSM.2\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche](#)

- [\[SSM.3\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [\[SSM.4\] SSM los documentos no deben ser públicos](#)
- [\[StepFunctions.1\] Las máquinas de estado de Step Functions deberían tener el registro activado](#)
- [\[StepFunctions.2\] Las actividades de Step Functions deben estar etiquetadas](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)
- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

Asia-Pacífico (Bombay)

Los siguientes controles no se admiten en Asia-Pacífico (Bombay).

- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[EC2.24\] No se deben usar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web 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 Asia-Pacífico (Osaka).

- [\[ACM.1\] Los certificados importados y ACM emitidos deben renovarse después de un período de tiempo específico](#)
- [\[Account.2\] Cuentas de AWS debe ser parte de una organización de AWS Organizations](#)
- [\[APIGateway.1\] La API puerta de enlace REST y el registro de WebSocket API ejecuciones deben estar habilitados](#)
- [\[APIGateway.2\] REST API Las etapas de la API puerta de enlace deben configurarse para usar SSL certificados para la autenticación de fondo](#)
- [\[APIGateway.3\] REST API Las etapas de API Gateway deben tener habilitado el AWS X-Ray rastreo](#)
- [\[APIGateway.4\] La API puerta de enlace debe estar asociada a una web WAF ACL](#)

- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[AutoScaling.5\] EC2 Las instancias de Amazon lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas](#)
- [Los puntos de recuperación de \[Backup.1\] AWS Backup deben estar cifrados en reposo](#)
- [\[Backup.4\] Los planes de informes de AWS Backup deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CloudWatch.15\] Las alarmas de CloudWatch deben tener configuradas acciones específicas](#)
- [\[CloudWatch.16\] Los grupos de registros de CloudWatch deben retenerse durante un periodo específico](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.7\] las tareas de DMS replicación de la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] las tareas de DMS replicación de la base de datos de origen deben tener el registro activado](#)

- [\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización 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](#)
- [\[DynamoDB.2\] Las tablas de DynamoDB deben tener habilitada la recuperación point-in-time](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.4\] 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 deberían poder restaurarse públicamente](#)
- [\[EC2.3\] Los volúmenes adjuntos de Amazon EBS deben cifrarse en reposo](#)
- [\[EC2.4\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.7\] 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](#)
- [\[EC2.13\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 22](#)
- [\[EC2.14\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 3389](#)
- [\[EC2.15\] EC2 Las subredes de Amazon no deberían 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 deberían permitir el tráfico entrante sin restricciones en los puertos autorizados](#)
- [\[EC2.20\] Los dos túneles VPN de una conexión AWS Site-to-Site VPN deben estar activos](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon no utilizados deberían eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC2.24\] No se deben usar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de respaldo](#)
- [\[EC2.51\] Los puntos finales de 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](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[ECS.1\] Las definiciones de ECS tareas de Amazon deben tener modos de red seguros y definiciones de usuario.](#)
- [\[ECS.9\] las definiciones de ECS tareas deben tener una configuración de registro](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] EFS Los volúmenes de Amazon deberían estar en los planes de respaldo](#)
- [\[ELB.1\] Application Load Balancer debe configurarse para redirigir todas las HTTP solicitudes a HTTPS](#)
- [\[ELB.2\] Los balanceadores de carga clásicos con HTTPS listenersSSL/deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.3\] Los oyentes de Classic Load Balancer deben configurarse con o con terminación HTTPS TLS](#)
- [\[ELB.4\] Application Load Balancer debe configurarse para eliminar los encabezados http no válidos](#)

- [\[ELB.6\] Los balanceadores de carga de aplicaciones, puertas de enlace y redes deben tener habilitada la protección contra eliminaciones](#)
- [\[ELB.8\] Los balanceadores de carga clásicos que utilizan dispositivos de SSL escucha deben usar una política de seguridad predefinida que tenga una larga duración AWS Config](#)
- [\[ELB.9\] Los balanceadores de carga clásicos deberían tener activado el balanceo de cargas entre zonas](#)
- [\[ELB.16\] Los balanceadores de carga de aplicaciones deben estar asociados a una web AWS WAF ACL](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(RedisOSS\) 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](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)
- [\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)
- [\[ES.1\] Los dominios de Elasticsearch deben tener habilitado el cifrado en reposo](#)
- [\[ES.3\] Los dominios de Elasticsearch deben cifrar los datos enviados entre nodos](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.4\] La clave de acceso del usuario raíz de IAM no debería existir](#)
- [\[IAM.18\] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte](#)
- [\[IAM.21\] Las políticas de IAM gestionadas por el cliente que usted cree no deberían permitir acciones comodín en los servicios](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[IoT.1\] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse](#)
- [\[IoT.2\] Las acciones de mitigación de AWS IoT Core deben etiquetarse](#)
- [\[IoT.3\] Las dimensiones de AWS IoT Core deben etiquetarse](#)
- [\[IoT.4\] Los autorizadores de AWS IoT Core deben etiquetarse](#)
- [\[IoT.5\] Los alias de los roles de AWS IoT Core deben etiquetarse](#)

- [\[IoT.6\] Las políticas de AWS IoT Core deben etiquetarse](#)
- [\[KMS.1\] 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](#)
- [\[Lambda.2\] Las funciones de Lambda deben usar los tiempos de ejecución admitidos](#)
- [\[Lambda.3\] Las funciones lambda deben estar en un VPC](#)
- [\[MSK.3\] Los conectores MSK Connect deben estar cifrados en tránsito](#)
- [\[RDS.1\] La instantánea de RDS debe ser privada](#)
- [Las instantáneas de clústeres y bases de datos de RDS \[RDS.4\] deben cifrarse cuando están inactivas](#)
- [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](#)
- [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](#)
- [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](#)
- [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](#)

- [\[Redshift.7\]](#) Los clústeres de Redshift deberían utilizar un enrutamiento mejorado VPC
- [Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo](#)
- [\[Route53.1\]](#) Las comprobaciones de estado de Route 53 deben estar etiquetadas
- [\[Route53.2\]](#) Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS
- [\[S3.8\]](#) Los buckets de uso general de S3 deben bloquear el 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
- [\[S3.24\]](#) Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público
- [\[SageMaker.1\]](#) Las instancias de Amazon SageMaker AI notebook no deberían tener acceso directo a Internet
- [\[SNS.1\]](#) SNS los temas deben cifrarse en reposo mediante AWS KMS
- [\[SSM.2\] EC2](#) Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche
- [\[SSM.3\] EC2](#) Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT
- [\[WAF.1\]](#) AWS WAF El ACL registro web global clásico debe estar habilitado
- [\[WAF.3\]](#) Los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla
- [\[WAF.6\]](#) Las reglas globales AWS WAF clásicas deben tener al menos una condición
- [\[WAF.7\]](#) Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla
- [\[WAF.8\]](#) La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas
- [\[WAF.10\]](#) la AWS WAF web ACLs debe tener al menos una regla o grupo de reglas
- [\[WAF.11\]](#) El ACL registro AWS WAF web debe estar habilitado
- [\[WorkSpaces.1\]](#) Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo
- [\[WorkSpaces.2\]](#) Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo

Asia-Pacífico (Seúl)

Los siguientes controles no se admiten en Asia-Pacífico (Seúl).

- [\[AppSync.1\]](#) las AWS AppSync API cachés deben cifrarse en reposo
- [\[AppSync.6\]](#) AWS AppSync API Las cachés deben cifrarse en tránsito

- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.24\] No se deben usar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)

- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web 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 Asia-Pacífico (Singapur).

- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)

- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web 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 Asia-Pacífico (Sídney).

- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)

- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

Asia-Pacífico (Tokio)

Los siguientes controles no se admiten en Asia-Pacífico (Tokio).

- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)

- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

Canadá (centro)

Los siguientes controles no se admiten en Canadá (centro).

- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.24\] No se deben usar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[Kinesis.3\] 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](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

China (Pekín)

Los siguientes controles no se admiten en China (Pekín).

- [\[ACM.1\] Los certificados importados y ACM emitidos deben renovarse después de un período de tiempo específico](#)
- [\[ACM.2\] RSA los certificados gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)
- [\[ACM.3\] ACM los certificados deben estar etiquetados](#)
- [\[Account.2\] Cuentas de AWS debe ser parte de una organización de AWS Organizations](#)

- [\[APIGateway.2\] REST API Las etapas de la API puerta de enlace deben configurarse para usar SSL certificados para la autenticación de fondo](#)
- [\[APIGateway.3\] REST API Las etapas de API Gateway deben tener habilitado el AWS X-Ray rastreo](#)
- [\[APIGateway.4\] La API puerta de enlace debe estar asociada a una web WAF ACL](#)
- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.4\] AWS AppSync APIs GraphQL debe estar etiquetado](#)
- [\[AppSync.6\] AWS AppSync API Las cachés 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](#)
- [\[AutoScaling.10\] Los grupos EC2 de Auto Scaling deben estar etiquetados](#)
- [Los puntos de recuperación de \[Backup.1\] AWS Backup deben estar cifrados en reposo](#)
- [\[Backup.2\] Los puntos de recuperación de AWS Backup deben etiquetarse](#)
- [\[Backup.3\] Los almacenes de AWS Backup deben etiquetarse](#)
- [\[Backup.4\] Los planes de informes de AWS Backup deben etiquetarse](#)
- [\[Backup.5\] Los planes de copias de seguridad de AWS Backup deben etiquetarse](#)
- [\[CloudFormation.2\] Las pilas de CloudFormation deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes y los orígenes personalizados](#)

- [\[CloudFront.13\] CloudFront las distribuciones deben usar el control de acceso al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CloudTrail.9\] las CloudTrail rutas deben estar etiquetadas](#)
- [\[CloudWatch.15\] Las alarmas de CloudWatch deben tener configuradas acciones específicas](#)
- [\[CloudWatch.16\] Los grupos de registros de CloudWatch deben retenerse durante un periodo específico](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[Cognito.1\] 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](#)
- [\[DataFirehose.1\] Los flujos de entrega de Firehose deben estar cifrados en reposo](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.2\] DMS los certificados deben estar etiquetados](#)
- [\[DMS.3\] las suscripciones a DMS eventos deben estar etiquetadas](#)
- [\[DMS.4\] las instancias de DMS replicación deben estar etiquetadas](#)
- [\[DMS.5\] los grupos de subredes de DMS replicación deben estar etiquetados](#)
- [\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización IAM](#)
- [\[DMS.11\] DMS Los puntos finales de MongoDB deberían tener habilitado un mecanismo de autenticación](#)
- [\[DMS.12\] DMS Los puntos finales de Redis deberían estar habilitados OSS TLS](#)
- [\[DocumentDB.1\] 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 \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)

- [\[DynamoDB.5\] Las tablas de DynamoDB deben etiquetarse](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.15\] EC2 Las subredes de Amazon no deberían asignar automáticamente direcciones IP públicas](#)
- [\[EC2.16\] Deben eliminarse las listas de control de acceso a la red no utilizadas](#)
- [\[EC2.20\] Los dos túneles VPN de una conexión AWS Site-to-Site VPN deben estar activos](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon no utilizados deberían 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 respaldo](#)
- [\[EC2.33\] Los archivos adjuntos a las pasarelas de EC2 tránsito deben estar etiquetados](#)
- [\[EC2.34\] Las tablas de rutas de las pasarelas de EC2 tránsito deben estar etiquetadas](#)
- [Las interfaces de EC2 red deben estar etiquetadas \[EC2.35\]](#)
- [\[EC2.36\] Las pasarelas de EC2 clientes deben estar etiquetadas](#)
- [\[EC2.37\] Las direcciones IP EC2 elásticas deben estar etiquetadas](#)
- [\[EC2.38\] EC2 las instancias deben estar etiquetadas](#)
- [\[EC2.39\] Las pasarelas EC2 de Internet deben estar etiquetadas](#)
- [\[EC2.40\] Las pasarelas EC2 NAT deben estar etiquetadas](#)
- [La EC2 red \[EC2.41\] ACLs debe estar etiquetada](#)
- [Las tablas de EC2 rutas deben estar etiquetadas \[EC2.42\]](#)
- [\[EC2.43\] 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 punto final de Amazon VPC deben estar etiquetados](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben estar etiquetados](#)
- [\[EC2.49\] Las conexiones de emparejamiento de Amazon VPC deben estar etiquetadas](#)
- [\[EC2.50\] Las pasarelas de EC2 VPN deben estar etiquetadas](#)
- [\[EC2.51\] Los puntos finales de EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)

- [\[EC2.52\] Las pasarelas de EC2 tránsito deben estar etiquetadas](#)
- [\[EC2.53\] los grupos de EC2 seguridad no deberían permitir la entrada desde el 0.0.0.0/0 a los puertos de administración remota del servidor](#)
- [\[EC2.54\] Los grupos EC2 de seguridad no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor](#)
- [\[EC2.58\] 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 activado](#)
- [\[ECR.1\] Los repositorios ECR privados deben tener configurado el escaneo de imágenes](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[ECS.1\] Las definiciones de ECS tareas de Amazon deben tener modos de red seguros y definiciones de usuario.](#)
- [\[ECS.13\] ECS los servicios deben estar etiquetados](#)
- [\[ECS.14\] los ECS clústeres deben estar etiquetados](#)
- [\[ECS.15\] Las definiciones de ECS tareas deben estar etiquetadas](#)
- [\[EFS.5\] los puntos de EFS acceso deben estar etiquetados](#)
- [\[EFS.6\] Los destinos de EFS montaje no deben estar asociados a una subred pública](#)
- [\[EKS.3\] los EKS clústeres deben usar secretos de Kubernetes cifrados](#)
- [\[EKS.6\] EKS los clústeres deben estar etiquetados](#)
- [\[EKS.7\] Las configuraciones de los proveedores de EKS identidad deben estar etiquetadas](#)
- [\[ELB.2\] Los balanceadores de carga clásicos con HTTPS listenersSSL/deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.16\] Los balanceadores de carga de aplicaciones deben estar asociados a una web AWS WAF ACL](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(RedisOSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElasticBeanstalk.1\] 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](#)
- [\[ES.3\] 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](#)
- [\[ES.9\] Los dominios de Elasticsearch deben estar etiquetados](#)
- [\[EventBridge.2\] los autobuses de EventBridge eventos deben estar etiquetados](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FSx.1\] FSx para sistemas de ZFS archivos abiertos, debe configurarse para copiar etiquetas a 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 etiquetarse](#)
- [\[Glue.1\] los AWS Glue trabajos deben estar etiquetados](#)
- [\[GuardDuty.1\] GuardDuty debe 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 del registro de GuardDuty EKS auditoría debe estar habilitada](#)
- [\[GuardDuty.6\] La protección GuardDuty Lambda debe estar habilitada](#)
- [\[GuardDuty.7\] La monitorización del GuardDuty EKS tiempo de ejecución debe estar habilitada](#)
- [\[GuardDuty.8\] La protección contra GuardDuty malware para EC2 debe estar habilitada](#)
- [\[GuardDuty.9\] La GuardDuty RDS protección debe estar habilitada](#)
- [\[GuardDuty.10\] La protección GuardDuty S3 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 la política adjunta 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 ECR escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.3\] 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](#)
- [\[IoT.1\] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse](#)
- [\[IoT.2\] Las acciones de mitigación de AWS IoT Core deben etiquetarse](#)
- [\[IoT.3\] Las dimensiones de AWS IoT Core deben etiquetarse](#)
- [\[IoT.4\] Los autorizadores de AWS IoT Core deben etiquetarse](#)
- [\[IoT.5\] Los alias de los roles de AWS IoT Core deben etiquetarse](#)
- [\[IoT.6\] Las políticas de AWS IoT Core deben etiquetarse](#)
- [\[Kinesis.2\] Las transmisiones de Kinesis deben etiquetarse](#)
- [\[Lambda.6\] 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 MSK Connect deben estar cifrados 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 bases de datos de Neptune deben tener habilitada la autenticación de bases de datos 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](#)
- [\[NetworkFirewall.1\] Los 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](#)
- [\[NetworkFirewall.7\] Los firewall de Network Firewall se deben etiquetar](#)
- [\[NetworkFirewall.8\] Las políticas de firewall de Network Firewall se deben etiquetar](#)
- [Los firewalls de Network Firewall \[NetworkFirewall.9\] 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](#)

- [Los OpenSearch dominios \[Opensearch.9\] deben estar etiquetados](#)
- [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 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](#)
- [\[Redshift.7\] Los clústeres de Redshift deberían utilizar un enrutamiento mejorado VPC](#)
- [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](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.1\] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[S3.8\] Los buckets de uso general de S3 deben bloquear el acceso público](#)
- [\[S3.14\] Los buckets de uso general de S3 deben tener habilitado el control de versiones](#)
- [\[S3.22\] 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 AI notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.4\] Las variantes de producción de terminales de SageMaker IA deben tener un recuento inicial de instancias superior a 1](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [\[SecretsManager.3\] 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 organización de AWS](#)

- [\[SNS.3\] SNS los temas deben estar etiquetados](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[StepFunctions.2\] Las actividades de Step Functions deben estar etiquetadas](#)
- [\[Transfer.1\] AWS Transfer Family Los flujos de trabajo deben estar etiquetados](#)
- [\[Transfer.2\] Los servidores Transfer Family no deben usar el FTP protocolo para la conexión de puntos finales](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.3\] Los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)
- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

China (Ningxia)

Los siguientes controles no se admiten en China (Ningxia).

- [\[ACM.1\] Los certificados importados y ACM emitidos deben renovarse después de un período de tiempo específico](#)
- [\[ACM.2\] RSA los certificados gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)
- [\[ACM.3\] ACM los certificados deben estar etiquetados](#)
- [\[Account.2\] Cuentas de AWS debe ser parte de una organización de AWS Organizations](#)
- [\[APIGateway.2\] REST API Las etapas de la API puerta de enlace deben configurarse para usar SSL certificados para la autenticación de fondo](#)
- [\[APIGateway.3\] REST API Las etapas de API Gateway deben tener habilitado el AWS X-Ray rastreo](#)
- [\[APIGateway.4\] La API puerta de enlace debe estar asociada a una web WAF ACL](#)
- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.4\] AWS AppSync APIs GraphQL debe estar etiquetado](#)

- [\[AppSync.6\] AWS AppSync API Las cachés 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](#)
- [\[AutoScaling.10\] Los grupos EC2 de Auto Scaling deben estar etiquetados](#)
- [Los puntos de recuperación de \[Backup.1\] AWS Backup deben estar cifrados en reposo](#)
- [\[Backup.2\] Los puntos de recuperación de AWS Backup deben etiquetarse](#)
- [\[Backup.3\] Los almacenes de AWS Backup deben etiquetarse](#)
- [\[Backup.4\] Los planes de informes de AWS Backup deben etiquetarse](#)
- [\[Backup.5\] Los planes de copias de seguridad de AWS Backup deben etiquetarse](#)
- [\[CloudFormation.2\] Las pilas de CloudFormation deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CloudTrail.9\] las CloudTrail rutas deben estar etiquetadas](#)
- [\[CloudWatch.15\] Las alarmas de CloudWatch deben tener configuradas acciones específicas](#)
- [\[CloudWatch.16\] Los grupos de registros de CloudWatch deben retenerse durante un periodo específico](#)

- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[Cognito.1\] 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](#)
- [\[DataFirehose.1\] Los flujos de entrega de Firehose deben estar cifrados en reposo](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.2\] DMS los certificados deben estar etiquetados](#)
- [\[DMS.3\] las suscripciones a DMS eventos deben estar etiquetadas](#)
- [\[DMS.4\] las instancias de DMS replicación deben estar etiquetadas](#)
- [\[DMS.5\] los grupos de subredes de DMS replicación deben estar etiquetados](#)
- [\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización IAM](#)
- [\[DMS.11\] DMS Los puntos finales de MongoDB deberían tener habilitado un mecanismo de autenticación](#)
- [\[DMS.12\] DMS Los puntos finales de Redis deberían estar habilitados OSS TLS](#)
- [\[DocumentDb.3\] Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.5\] Las tablas de DynamoDB deben etiquetarse](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.15\] EC2 Las subredes de Amazon no deberían asignar automáticamente direcciones IP públicas](#)
- [\[EC2.16\] Deben eliminarse las listas de control de acceso a la red no utilizadas](#)
- [\[EC2.20\] Los dos túneles VPN de una conexión AWS Site-to-Site VPN deben estar activos](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon no utilizados deberían eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC2.24\] No se deben usar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[EC2.28\] Los volúmenes de EBS deben estar cubiertos por un plan de respaldo](#)
- [\[EC2.33\] Los archivos adjuntos a las pasarelas de EC2 tránsito deben estar etiquetados](#)
- [\[EC2.34\] Las tablas de rutas de las pasarelas de EC2 tránsito deben estar etiquetadas](#)

- [Las interfaces de EC2 red deben estar etiquetadas \[EC2.35\]](#)
- [\[EC2.36\] Las pasarelas de EC2 clientes deben estar etiquetadas](#)
- [\[EC2.37\] Las direcciones IP EC2 elásticas deben estar etiquetadas](#)
- [\[EC2.38\] EC2 las instancias deben estar etiquetadas](#)
- [\[EC2.39\] Las pasarelas EC2 de Internet deben estar etiquetadas](#)
- [\[EC2.40\] Las pasarelas EC2 NAT deben estar etiquetadas](#)
- [La EC2 red \[EC2.41\] ACLs debe estar etiquetada](#)
- [Las tablas de EC2 rutas deben estar etiquetadas \[EC2.42\]](#)
- [\[EC2.43\] 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 punto final de Amazon VPC deben estar etiquetados](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben estar etiquetados](#)
- [\[EC2.49\] Las conexiones de emparejamiento de Amazon VPC deben estar etiquetadas](#)
- [\[EC2.50\] Las pasarelas de EC2 VPN deben estar etiquetadas](#)
- [\[EC2.51\] Los puntos finales de EC2 Client VPN deben tener habilitado el registro de conexiones de clientes](#)
- [\[EC2.52\] Las pasarelas de EC2 tránsito 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](#)
- [\[EC2.171\] Las conexiones EC2 VPN deben tener el registro activado](#)
- [\[ECR.1\] Los repositorios ECR privados deben tener configurado el escaneo de imágenes](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[ECS.1\] Las definiciones de ECS tareas de Amazon deben tener modos de red seguros y definiciones de usuario.](#)
- [\[ECS.13\] ECS los servicios deben estar etiquetados](#)
- [\[ECS.14\] los ECS clústeres deben estar etiquetados](#)

- [\[ECS.15\] Las definiciones de ECS tareas deben estar etiquetadas](#)
- [\[EFS.3\] los puntos de EFS acceso deben establecer un directorio raíz](#)
- [\[EFS.4\] los puntos de EFS acceso deben imponer la identidad de un usuario](#)
- [\[EFS.5\] los puntos de EFS acceso deben estar etiquetados](#)
- [\[EFS.6\] Los destinos de EFS montaje no deben estar asociados a una subred pública](#)
- [\[EKS.3\] los EKS clústeres deben usar secretos de Kubernetes cifrados](#)
- [\[EKS.6\] EKS los clústeres deben estar etiquetados](#)
- [\[EKS.7\] Las configuraciones de los proveedores de EKS identidad deben estar etiquetadas](#)
- [\[ELB.2\] Los balanceadores de carga clásicos con HTTPS listenersSSL/deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.16\] Los balanceadores de carga de aplicaciones deben estar asociados a una web AWS WAF ACL](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(RedisOSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElasticBeanstalk.1\] 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](#)
- [\[ES.1\] Los dominios de Elasticsearch deben tener habilitado el cifrado 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](#)
- [\[ES.9\] Los dominios de Elasticsearch deben estar etiquetados](#)
- [\[EventBridge.2\] los autobuses de EventBridge eventos deben estar etiquetados](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[FSx.1\] FSx para sistemas de ZFS archivos abiertos, debe configurarse para copiar etiquetas a 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 etiquetarse](#)
- [\[Glue.1\] los AWS Glue trabajos deben estar etiquetados](#)
- [\[Glue.3\] Las transformaciones AWS Glue de aprendizaje automático deben cifrarse en reposo](#)
- [\[GuardDuty.1\] GuardDuty debe 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 del registro de GuardDuty EKS auditoría debe estar habilitada](#)
- [\[GuardDuty.6\] La protección GuardDuty Lambda debe estar habilitada](#)
- [\[GuardDuty.7\] La monitorización del GuardDuty EKS tiempo de ejecución debe estar habilitada](#)
- [\[GuardDuty.8\] La protección contra GuardDuty malware para EC2 debe estar habilitada](#)
- [\[GuardDuty.9\] La GuardDuty RDS protección debe estar habilitada](#)
- [\[GuardDuty.10\] La protección GuardDuty S3 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 la política adjunta 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 ECR escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.3\] 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](#)
- [\[IoT.1\] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse](#)
- [\[IoT.2\] Las acciones de mitigación de AWS IoT Core deben etiquetarse](#)
- [\[IoT.3\] Las dimensiones de AWS IoT Core deben etiquetarse](#)

- [\[IoT.4\] Los autorizadores de AWS IoT Core deben etiquetarse](#)
- [\[IoT.5\] Los alias de los roles de AWS IoT Core deben etiquetarse](#)
- [\[IoT.6\] Las políticas de AWS IoT Core deben etiquetarse](#)
- [\[Kinesis.2\] Las transmisiones de Kinesis deben etiquetarse](#)
- [\[Lambda.1\] 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 lambda deben estar en un VPC](#)
- [\[Lambda.5\] Las funciones VPC Lambda 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 MSK Connect deben estar cifrados en tránsito](#)
- [\[Neptune.3\] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas](#)
- [\[NetworkFirewall.1\] Los 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](#)
- [\[NetworkFirewall.7\] Los firewall de Network Firewall se deben etiquetar](#)
- [\[NetworkFirewall.8\] Las políticas de firewall de Network Firewall se deben etiquetar](#)
- [Los firewalls de Network Firewall \[NetworkFirewall.9\] 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](#)
- [Los OpenSearch dominios \[Opensearch.9\] deben estar etiquetados](#)
- [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 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](#)
- [Los clústeres de Amazon Redshift \[Redshift.3\] deben tener habilitadas las instantáneas automáticas](#)
- [\[Redshift.7\] Los clústeres de Redshift deberían utilizar un enrutamiento mejorado VPC](#)
- [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](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.1\] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[S3.8\] Los buckets de uso general de S3 deben bloquear el acceso público](#)
- [\[S3.14\] Los buckets de uso general de S3 deben tener habilitado el control de versiones](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker AI notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.4\] Las variantes de producción de terminales de SageMaker IA deben tener un recuento inicial de instancias superior a 1](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [\[SecretsManager.3\] 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 organización de AWS](#)
- [\[SNS.3\] SNS los temas deben estar etiquetados](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[StepFunctions.2\] Las actividades de Step Functions deben estar etiquetadas](#)
- [\[Transfer.1\] AWS Transfer Family Los flujos de trabajo deben estar etiquetados](#)
- [\[Transfer.2\] Los servidores Transfer Family no deben usar el FTP protocolo para la conexión de puntos finales](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.3\] Los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado](#)

Europa (Fráncfort)

Los siguientes controles no se admiten en Europa (Fráncfort).

- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)

- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.26\] 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](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

Europa (Irlanda)

Los siguientes controles no se admiten en Europa (Irlanda).

- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)

- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

Europa (Londres)

Los siguientes controles no se admiten en Europa (Londres).

- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)

- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[EC2.24\] No se deben usar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.26\] 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](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

Europa (Milán)

Los siguientes controles no se admiten en Europa (Milán).

- [\[ACM.1\] Los certificados importados y ACM emitidos deben renovarse después de un período de tiempo específico](#)
- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CodeBuild.1\] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales](#)
- [\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)
- [\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización IAM](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.3\] Los volúmenes adjuntos de Amazon EBS deben cifrarse en reposo](#)
- [\[EC2.4\] 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](#)
- [\[EC2.12\] Amazon no utilizado EC2 EIPs debería retirarse](#)
- [\[EC2.13\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 22](#)
- [\[EC2.14\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 3389](#)
- [\[EC2.24\] No se deben usar 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](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] EFS Los volúmenes de Amazon deberían estar en los planes de respaldo](#)
- [\[ELB.1\] Application Load Balancer debe configurarse para redirigir todas las HTTP solicitudes a HTTPS](#)
- [\[ELB.2\] Los balanceadores de carga clásicos con HTTPS listenersSSL/deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.4\] Application Load Balancer debe configurarse para eliminar los encabezados http no válidos](#)
- [\[ELB.8\] Los balanceadores de carga clásicos que utilizan dispositivos de SSL escucha deben usar una política de seguridad predefinida que tenga una larga duración AWS Config](#)
- [\[ELB.16\] Los balanceadores de carga de aplicaciones deben estar asociados a una web AWS WAF ACL](#)
- [\[EMR.1\] Los nodos maestros del clúster de Amazon EMR no deben tener direcciones IP públicas](#)
- [\[ES.3\] 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](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.18\] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte](#)

- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[IoT.1\] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse](#)
- [\[IoT.2\] Las acciones de mitigación de AWS IoT Core deben etiquetarse](#)
- [\[IoT.3\] Las dimensiones de AWS IoT Core deben etiquetarse](#)
- [\[IoT.4\] Los autorizadores de AWS IoT Core deben etiquetarse](#)
- [\[IoT.5\] Los alias de los roles de AWS IoT Core deben etiquetarse](#)
- [\[IoT.6\] Las políticas de AWS IoT Core deben etiquetarse](#)
- [\[MSK.3\] Los conectores MSK Connect deben estar cifrados 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 bases de datos de Neptune deben tener habilitada la autenticación de bases de datos 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](#)
- [Las instantáneas de clústeres y bases de datos de RDS \[RDS.4\] deben cifrarse cuando están inactivas](#)
- [\[RDS.9\] Las instancias de base de datos de RDS deben publicar los registros en Logs CloudWatch](#)
- [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](#)

- [\[Redshift.2\] Las conexiones a los clústeres de Amazon Redshift \[Redshift.2\] deben cifrarse en tránsito](#)
- [\[Redshift.3\] Los clústeres de Amazon Redshift \[Redshift.3\] deben tener habilitadas las instantáneas automáticas](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas 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 AI notebook no deberían tener acceso directo a Internet](#)
- [\[SSM.2\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche](#)
- [\[SSM.3\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)
- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

Europa (París)

Los siguientes controles no se admiten en Europa (París).

- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)

- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[EC2.24\] No se deben usar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)
- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

Europa (España)

Los siguientes controles no se admiten en Europa (España).

- [\[ACM.1\] Los certificados importados y ACM emitidos deben renovarse después de un período de tiempo específico](#)
- [\[Account.2\] Cuentas de AWS debe ser parte de una organización de AWS Organizations](#)
- [\[APIGateway.3\] REST API Las etapas de API Gateway deben tener habilitado el AWS X-Ray rastreo](#)
- [\[APIGateway.4\] La API puerta de enlace debe estar asociada a una web WAF ACL](#)
- [\[APIGateway.8\] Las rutas de API gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas de API Gateway V2](#)
- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[Athena.4\] Los grupos de trabajo de Athena deben tener el registro habilitado](#)
- [Los puntos de recuperación de \[Backup.1\] AWS Backup deben estar cifrados en reposo](#)
- [\[Backup.2\] Los puntos de recuperación de AWS Backup deben etiquetarse](#)
- [\[Backup.4\] Los planes de informes de AWS Backup deben etiquetarse](#)
- [\[CloudFormation.2\] Las pilas de CloudFormation deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)

- [\[CloudTrail.6\] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público](#)
- [\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3](#)
- [\[CloudWatch.16\] Los grupos de registros de CloudWatch deben retenerse durante un periodo específico](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[CodeBuild.1\] 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](#)
- [\[CodeBuild.7\] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo](#)
- [\[Cognito.1\] 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](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)
- [\[DMS.2\] DMS los certificados deben estar etiquetados](#)
- [\[DMS.3\] las suscripciones a DMS eventos deben estar etiquetadas](#)
- [\[DMS.4\] las instancias de DMS replicación deben estar etiquetadas](#)
- [\[DMS.5\] los grupos de subredes de DMS replicación deben estar etiquetados](#)
- [\[DMS.6\] las instancias de DMS replicación deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] las tareas de DMS replicación de la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] las tareas de DMS replicación de la base de datos de origen deben tener el registro activado](#)
- [\[DMS.9\] Los DMS puntos finales deben utilizar SSL](#)
- [\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización IAM](#)
- [\[DMS.11\] DMS Los puntos finales de MongoDB deberían tener habilitado un mecanismo de autenticación](#)
- [\[DMS.12\] DMS Los puntos finales de Redis deberían estar habilitados OSS TLS](#)

- [\[DocumentDB.1\] 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 \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.4\] 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 deberían poder restaurarse públicamente](#)
- [\[EC2.2\] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente](#)
- [\[EC2.3\] Los volúmenes adjuntos de Amazon EBS deben cifrarse en reposo](#)
- [\[EC2.4\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.6\] El registro de flujo de VPC debe estar habilitado en todas 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](#)
- [\[EC2.13\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 22](#)
- [\[EC2.14\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 3389](#)
- [\[EC2.15\] EC2 Las subredes de Amazon no deberían 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 deberían permitir el tráfico entrante sin restricciones en los puertos autorizados](#)
- [\[EC2.20\] Los dos túneles VPN de una conexión AWS Site-to-Site VPN deben estar activos](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon no utilizados deberían eliminarse](#)
- [\[EC2.24\] No se deben usar 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 respaldo](#)
- [\[EC2.34\] Las tablas de rutas de las pasarelas de EC2 tránsito deben estar etiquetadas](#)
- [\[EC2.40\] Las pasarelas EC2 NAT deben estar etiquetadas](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben estar etiquetados](#)
- [\[EC2.51\] Los puntos finales de 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 utilizar la versión 2 \(\) del Servicio de Metadatos de Instancia IMDSv2](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[ECS.9\] las definiciones de ECS tareas deben tener una configuración de registro](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] EFS Los volúmenes de Amazon deberían estar en los planes de respaldo](#)
- [\[ELB.1\] Application Load Balancer debe configurarse para redirigir todas las HTTP solicitudes a HTTPS](#)
- [\[ELB.2\] Los balanceadores de carga clásicos con HTTPS listenersSSL/deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.3\] Los oyentes de Classic Load Balancer deben configurarse con o con terminación HTTPS TLS](#)

- [\[ELB.4\] Application Load Balancer debe configurarse para eliminar los encabezados http no válidos](#)
- [\[ELB.5\] El registro de aplicaciones y balanceadores de carga clásicos debe estar habilitado](#)
- [\[ELB.6\] Los balanceadores de carga de aplicaciones, puertas de enlace y redes deben tener habilitada la protección contra eliminaciones](#)
- [\[ELB.8\] Los balanceadores de carga clásicos que utilizan dispositivos de SSL escucha deben usar una política de seguridad predefinida que tenga una larga duración AWS Config](#)
- [\[ELB.9\] Los balanceadores de carga clásicos deberían tener activado el balanceo de cargas entre zonas](#)
- [\[ELB.14\] El Classic Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.16\] Los balanceadores de carga de aplicaciones deben estar asociados a una web AWS WAF ACL](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(RedisOSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(RedisOSS\) de versiones anteriores deberían tener Redis activado OSS AUTH](#)
- [\[ElastiCache.7\] 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](#)
- [\[ES.1\] 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](#)
- [\[EventBridge.3\] 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](#)

- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[Glue.1\] los AWS Glue trabajos deben estar etiquetados](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[GuardDuty.3\] GuardDuty IPSets debe estar etiquetado](#)
- [\[GuardDuty.9\] La GuardDuty RDS protección 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](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.18\] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte](#)
- [\[IAM.19\] 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 la política adjunta AWSCloud ShellFullAccess](#)
- [\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.2\] El ECR escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.3\] 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](#)
- [\[IoT.1\] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse](#)
- [\[IoT.2\] Las acciones de mitigación de AWS IoT Core deben etiquetarse](#)
- [\[IoT.3\] Las dimensiones de AWS IoT Core deben etiquetarse](#)

- [\[IoT.4\] Los autorizadores de AWS IoT Core deben etiquetarse](#)
- [\[IoT.5\] Los alias de los roles de AWS IoT Core deben etiquetarse](#)
- [\[IoT.6\] Las políticas de AWS IoT Core deben etiquetarse](#)
- [\[KMS.1\] 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](#)
- [\[Lambda.1\] 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 lambda deben estar en un VPC](#)
- [\[Macie.1\] 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 MSK Connect deben estar cifrados 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 bases de datos de Neptune deben tener habilitada la autenticación de bases de datos 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](#)
- [\[RDS.2\] 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](#)
- [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](#)
- [\[Redshift.1\] 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](#)
- [Amazon Redshift \[Redshift.6\] debería tener habilitadas las actualizaciones automáticas a las versiones principales](#)
- [\[Redshift.7\] Los clústeres de Redshift deberían utilizar un enrutamiento mejorado VPC](#)
- [Los clústeres de Redshift \[Redshift.10\] deben cifrarse en reposo](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.1\] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[S3.5\] Los depósitos de uso general de S3 deberían requerir solicitudes de uso 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](#)
- [\[S3.15\] 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](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker AI notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] Las instancias de SageMaker AI notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker AI Notebook](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [\[SNS.1\] SNS los temas deben cifrarse en reposo mediante AWS KMS](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SSM.1\] EC2 Las instancias de Amazon deben gestionarse mediante AWS Systems Manager](#)
- [\[SSM.2\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche](#)
- [\[SSM.3\] EC2 Las instancias de Amazon gestionadas 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](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.3\] Los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.10\] la AWS WAF web ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)
- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

Europa (Estocolmo)

Los siguientes controles no se admiten en Europa (Estocolmo).

- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[DocumentDB.1\] 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 \(\) deben cifrarse en reposo DAX](#)

- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.24\] No se deben usar los tipos de instancias EC2 paravirtuales de Amazon](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [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](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)
- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

Europa (Zúrich)

Los siguientes controles no se admiten en Europa (Zúrich).

- [\[ACM.1\] Los certificados importados y ACM emitidos deben renovarse después de un período de tiempo específico](#)
- [\[APIGateway.8\] Las rutas de API gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas de API Gateway V2](#)
- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[Athena.4\] Los grupos de trabajo de Athena deben tener el registro habilitado](#)
- [Los puntos de recuperación de \[Backup.1\] AWS Backup deben estar cifrados en reposo](#)

- [\[Backup.2\] Los puntos de recuperación de AWS Backup deben etiquetarse](#)
- [\[Backup.4\] Los planes de informes de AWS Backup deben etiquetarse](#)
- [\[CloudFormation.2\] Las pilas de CloudFormation deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CloudTrail.6\] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público](#)
- [\[CloudTrail.7\] Asegúrese de que el registro de acceso al bucket de S3 esté habilitado en el CloudTrail bucket de S3](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[CodeBuild.1\] 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](#)
- [\[CodeBuild.7\] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo](#)
- [\[Cognito.1\] 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](#)

- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)
- [\[DMS.2\] DMS los certificados deben estar etiquetados](#)
- [\[DMS.3\] las suscripciones a DMS eventos deben estar etiquetadas](#)
- [\[DMS.4\] las instancias de DMS replicación deben estar etiquetadas](#)
- [\[DMS.5\] los grupos de subredes de DMS replicación deben estar etiquetados](#)
- [\[DMS.6\] las instancias de DMS replicación deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] las tareas de DMS replicación de la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] las tareas de DMS replicación de la base de datos de origen deben tener el registro activado](#)
- [\[DMS.9\] Los DMS puntos finales deben utilizar SSL](#)
- [\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización IAM](#)
- [\[DMS.11\] DMS Los puntos finales de MongoDB deberían tener habilitado un mecanismo de autenticación](#)
- [\[DMS.12\] DMS Los puntos finales de Redis deberían estar habilitados OSS TLS](#)
- [\[DocumentDB.1\] 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 \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.4\] 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](#)
- [\[EC2.2\] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente](#)
- [\[EC2.3\] Los volúmenes adjuntos de Amazon EBS deben cifrarse en reposo](#)
- [\[EC2.4\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.6\] El registro de flujo de VPC debe estar habilitado en todas VPCs](#)
- [\[EC2.8\] 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](#)
- [\[EC2.13\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 22](#)
- [\[EC2.14\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 3389](#)
- [\[EC2.15\] EC2 Las subredes de Amazon no deberían 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 deberían permitir el tráfico entrante sin restricciones en los puertos autorizados](#)
- [\[EC2.20\] Los dos túneles VPN de una conexión AWS Site-to-Site VPN deben estar activos](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon no utilizados deberían eliminarse](#)
- [\[EC2.24\] No se deben usar 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 respaldo](#)
- [\[EC2.51\] Los puntos finales de 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 utilizar la versión 2 \(\) del Servicio de Metadatos de Instancia IMDSv2](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[ECS.9\] las definiciones de ECS tareas deben tener una configuración de registro](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] EFS Los volúmenes de Amazon deberían estar en los planes de respaldo](#)
- [\[ELB.1\] Application Load Balancer debe configurarse para redirigir todas las HTTP solicitudes a HTTPS](#)
- [\[ELB.2\] Los balanceadores de carga clásicos con HTTPS listenersSSL/deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.3\] Los oyentes de Classic Load Balancer deben configurarse con o con terminación HTTPS TLS](#)
- [\[ELB.4\] Application Load Balancer debe configurarse para eliminar los encabezados http no válidos](#)
- [\[ELB.8\] Los balanceadores de carga clásicos que utilizan dispositivos de SSL escucha deben usar una política de seguridad predefinida que tenga una larga duración AWS Config](#)
- [\[ELB.9\] Los balanceadores de carga clásicos deberían tener activado el balanceo de cargas entre zonas](#)
- [\[ELB.14\] El Classic Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.16\] Los balanceadores de carga de aplicaciones deben estar asociados a una web AWS WAF ACL](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(RedisOSS\) deben tener habilitadas las copias de seguridad automáticas](#)
- [\[ElastiCache.6\] Los grupos de replicación ElastiCache \(RedisOSS\) de versiones anteriores deberían tener Redis activado OSS AUTH](#)
- [\[ElastiCache.7\] 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](#)

- [\[ES.1\] 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](#)
- [\[EventBridge.3\] 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](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[Glue.1\] los AWS Glue trabajos deben estar etiquetados](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[GuardDuty.3\] GuardDuty IP Sets debe estar etiquetado](#)
- [\[GuardDuty.9\] La GuardDuty RDS protección 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](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.18\] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte](#)
- [\[IAM.19\] 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 la política adjunta AWSCloud ShellFullAccess](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[IoT.1\] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse](#)
- [\[IoT.2\] Las acciones de mitigación de AWS IoT Core deben etiquetarse](#)
- [\[IoT.3\] Las dimensiones de AWS IoT Core deben etiquetarse](#)
- [\[IoT.4\] Los autorizadores de AWS IoT Core deben etiquetarse](#)
- [\[IoT.5\] Los alias de los roles de AWS IoT Core deben etiquetarse](#)
- [\[IoT.6\] Las políticas de AWS IoT Core deben etiquetarse](#)
- [\[KMS.1\] 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 MSK Connect deben estar cifrados 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 bases de datos de Neptune deben tener habilitada la autenticación de bases de datos 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](#)
- [\[RDS.3\] Las instancias de base de datos de RDS deben tener habilitado el cifrado en reposo](#)
- [Las instancias de base de datos de RDS \[RDS.5\] deben configurarse con varias zonas de disponibilidad](#)
- [Las instancias de base de datos de RDS \[RDS.8\] deben tener habilitada la protección contra la eliminación](#)
- [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 clústeres de Amazon Redshift \[Redshift.3\] deben tener habilitadas las instantáneas automáticas](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.1\] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[S3.8\] Los buckets de uso general de S3 deben bloquear el 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 AI notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] Las instancias de SageMaker AI notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker AI Notebook](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [\[SNS.1\] SNS los temas deben cifrarse en reposo mediante AWS KMS](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SSM.2\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche](#)
- [\[SSM.3\] EC2 Las instancias de Amazon gestionadas 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](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.3\] Los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.10\] la AWS WAF web ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)

- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

Israel (Tel Aviv)

Los siguientes controles no se admiten en Israel (Tel Aviv).

- [\[ACM.1\] Los certificados importados y ACM emitidos deben renovarse después de un período de tiempo específico](#)
- [\[APIGateway.8\] Las rutas de API gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas de API Gateway V2](#)
- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.2\] AWS AppSync debe tener activado el registro a nivel de campo](#)
- [\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves API](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[Athena.4\] Los grupos de trabajo de Athena deben tener el registro habilitado](#)
- [\[AutoScaling.5\] EC2 Las instancias de Amazon lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas](#)
- [Los puntos de recuperación de \[Backup.1\] AWS Backup deben estar cifrados en reposo](#)
- [\[Backup.2\] Los puntos de recuperación de AWS Backup deben etiquetarse](#)
- [\[Backup.4\] Los planes de informes de AWS Backup deben etiquetarse](#)
- [\[CloudFormation.2\] Las pilas de CloudFormation deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)

- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[CodeBuild.1\] 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](#)
- [\[CodeBuild.7\] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo](#)
- [\[DataSync.1\] Las tareas de DataSync deben tener el registro habilitado](#)
- [\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)
- [\[DMS.2\] DMS los certificados deben estar etiquetados](#)
- [\[DMS.3\] las suscripciones a DMS eventos deben estar etiquetadas](#)
- [\[DMS.4\] las instancias de DMS replicación deben estar etiquetadas](#)
- [\[DMS.5\] los grupos de subredes de DMS replicación deben estar etiquetados](#)
- [\[DMS.6\] las instancias de DMS replicación deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] las tareas de DMS replicación de la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] las tareas de DMS replicación de la base de datos de origen deben tener el registro activado](#)
- [\[DMS.9\] Los DMS puntos finales deben utilizar SSL](#)
- [\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización IAM](#)
- [\[DMS.11\] DMS Los puntos finales de MongoDB deberían tener habilitado un mecanismo de autenticación](#)
- [\[DMS.12\] DMS Los puntos finales de Redis deberían estar habilitados OSS TLS](#)
- [\[DocumentDB.1\] 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 \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.4\] 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](#)
- [\[EC2.3\] Los volúmenes adjuntos de Amazon EBS deben cifrarse en reposo](#)
- [\[EC2.4\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.6\] El registro de flujo de VPC debe estar habilitado en todas 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 deberían permitir la entrada desde el 0.0.0.0/0 o :/0 al puerto 22](#)
- [\[EC2.14\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o :/0 al puerto 3389](#)
- [\[EC2.18\] Los grupos de seguridad solo deberían permitir el tráfico entrante sin restricciones en los puertos autorizados](#)
- [\[EC2.20\] Los dos túneles VPN de una conexión AWS Site-to-Site VPN deben estar activos](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon no utilizados deberían eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC2.24\] No se deben usar 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 respaldo](#)
- [\[EC2.33\] Los archivos adjuntos a las pasarelas de EC2 tránsito deben estar etiquetados](#)
- [\[EC2.34\] Las tablas de rutas de las pasarelas de EC2 tránsito deben estar etiquetadas](#)
- [\[EC2.40\] Las pasarelas EC2 NAT deben estar etiquetadas](#)

- [\[EC2.48\] Los registros de flujo de Amazon VPC deben estar etiquetados](#)
- [\[EC2.51\] Los puntos finales de 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 utilizar la versión 2 \(\) del Servicio de Metadatos de Instancia IMDSv2](#)
- [\[ECR.2\] Los repositorios ECR privados deben tener configurada la inmutabilidad de las etiquetas](#)
- [\[ECR.3\] ECR Los repositorios deben tener configurada al menos una política de ciclo de vida](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[ECS.1\] Las definiciones de ECS tareas de Amazon deben tener modos de red seguros y definiciones de usuario.](#)
- [\[ECS.9\] las definiciones de ECS tareas deben tener una configuración de registro](#)
- [\[ECS.16\] Los conjuntos de ECS tareas 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](#)
- [\[EFS.2\] EFS Los volúmenes de Amazon deberían estar en los planes de respaldo](#)
- [\[EFS.3\] los puntos de EFS acceso deben establecer un directorio raíz](#)
- [\[EFS.4\] los puntos de EFS acceso deben imponer la identidad de un usuario](#)
- [\[EFS.6\] Los destinos de EFS montaje no deben estar asociados a una subred pública](#)
- [\[EFS.7\] los sistemas de EFS archivos deben tener habilitadas las copias de seguridad automáticas](#)
- [\[EFS.8\] los sistemas de EFS archivos deben cifrarse en reposo](#)
- [\[EKS.2\] EKS los clústeres deberían ejecutarse en una versión compatible de Kubernetes](#)
- [\[EKS.6\] EKS los clústeres deben estar etiquetados](#)
- [\[EKS.7\] Las configuraciones de los proveedores de EKS identidad deben estar etiquetadas](#)
- [\[EKS.8\] EKS los clústeres deben tener habilitado el registro de auditoría](#)

- [\[ELB.1\] Application Load Balancer debe configurarse para redirigir todas las HTTP solicitudes a HTTPS](#)
- [\[ELB.2\] Los balanceadores de carga clásicos con HTTPS listenersSSL/deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.4\] Application Load Balancer debe configurarse para eliminar los encabezados http no válidos](#)
- [\[ELB.6\] Los balanceadores de carga de aplicaciones, puertas de enlace y redes deben tener habilitada la protección contra eliminaciones](#)
- [\[ELB.8\] Los balanceadores de carga clásicos que utilizan dispositivos de SSL escucha deben usar una política de seguridad predefinida que tenga una larga duración AWS Config](#)
- [\[ELB.14\] El Classic Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.16\] Los balanceadores de carga de aplicaciones deben estar asociados a una web AWS WAF ACL](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(RedisOSS\) 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 \(RedisOSS\) de versiones anteriores deberían tener Redis activado OSS AUTH](#)
- [\[ElastiCache.7\] 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](#)
- [\[ES.1\] 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](#)
- [\[EventBridge.3\] 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](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[GuardDuty.1\] GuardDuty debe estar activado](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)
- [\[GuardDuty.3\] GuardDuty IPSets debe estar etiquetado](#)
- [\[GuardDuty.9\] La GuardDuty RDS protección 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 para los usuarios de IAM deben tener una duración estricta AWS Config](#)
- [\[IAM.11\] 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](#)
- [\[IAM.18\] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte](#)
- [\[IAM.19\] 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 la política adjunta 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 ECR escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.3\] 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](#)
- [\[IoT.1\] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse](#)
- [\[IoT.2\] Las acciones de mitigación de AWS IoT Core deben etiquetarse](#)
- [\[IoT.3\] Las dimensiones de AWS IoT Core deben etiquetarse](#)
- [\[IoT.4\] Los autorizadores de AWS IoT Core deben etiquetarse](#)
- [\[IoT.5\] Los alias de los roles de AWS IoT Core deben etiquetarse](#)
- [\[IoT.6\] Las políticas de AWS IoT Core deben etiquetarse](#)
- [\[Kinesis.1\] 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 VPC Lambda 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](#)
- [\[MSK.1\] MSK Los clústeres deben cifrarse en tránsito entre los nodos intermediarios](#)
- [\[MSK.2\] MSK los clústeres deben tener configurada una supervisión mejorada](#)
- [\[MSK.3\] Los conectores MSK Connect deben estar cifrados 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 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 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](#)
- [La autenticación de IAM \[RDS.12\] debe configurarse para los clústeres de RDS](#)
- [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](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas 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](#)
- [\[S3.8\] 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](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker AI notebook no deberían tener acceso directo a Internet](#)

- [\[SageMaker.2\] Las instancias de SageMaker AI notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker AI Notebook](#)
- [\[ServiceCatalog.1\] Las carteras de Service Catalog solo deben compartirse dentro de una organización de AWS](#)
- [\[SNS.1\] SNS los temas deben cifrarse en reposo mediante AWS KMS](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SSM.1\] EC2 Las instancias de Amazon deben gestionarse mediante AWS Systems Manager](#)
- [\[SSM.2\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche](#)
- [\[SSM.3\] EC2 Las instancias de Amazon gestionadas por Systems Manager deben tener un estado de conformidad de asociación de COMPLIANT](#)
- [\[SSM.4\] SSM los documentos no deben ser públicos](#)
- [\[StepFunctions.1\] Las máquinas de estado de Step Functions deberían tener el registro activado](#)
- [\[StepFunctions.2\] Las actividades de Step Functions deben estar etiquetadas](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.3\] Los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)
- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

Medio Oriente (Baréin)

Los siguientes controles no se admiten en Medio Oriente (Baréin).

- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)

- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[DocumentDB.1\] 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 \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.20\] Los dos túneles VPN de una conexión AWS Site-to-Site VPN deben estar activos](#)
- [\[EC2.24\] No se deben usar 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](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk debería transmitir los registros a CloudWatch](#)
- [\[EventBridge.4\] Los puntos finales EventBridge globales deberían tener habilitada la replicación de eventos](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[GuardDuty.1\] GuardDuty debe estar activado](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)
- [\[MSK.3\] Los conectores MSK Connect deben estar cifrados en tránsito](#)
- [Los clústeres de RDS \[RDS.7\] deben tener habilitada la protección contra la eliminación](#)
- [La autenticación de IAM \[RDS.12\] debe configurarse para los clústeres de RDS](#)
- [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](#)
- [\[RDS.31\] Los grupos de seguridad de bases de datos de RDS deben etiquetarse](#)
- [Amazon Redshift \[Redshift.6\] debería tener habilitadas las actualizaciones automáticas a las versiones principales](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas 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 de Amazon gestionadas por Systems Manager deben tener un estado de conformidad con el parche COMPLIANT tras la instalación de un parche](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)
- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

Oriente Medio (UAE)

Los siguientes controles no se admiten en Oriente Medio (UAE).

- [\[APIGateway.8\] Las rutas de API gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas de API Gateway V2](#)
- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.6\] AWS AppSync API Las cachés deben cifrarse en tránsito](#)
- [\[AutoScaling.1\] Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar controles de ELB estado](#)
- [Los puntos de recuperación de \[Backup.1\] AWS Backup deben estar cifrados en reposo](#)
- [\[Backup.2\] Los puntos de recuperación de AWS Backup deben etiquetarse](#)
- [\[Backup.4\] Los planes de informes de AWS Backup deben etiquetarse](#)
- [\[CloudFormation.2\] Las pilas de CloudFormation deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CloudTrail.1\] CloudTrail debe habilitarse y configurarse con al menos un registro multirregional que incluya eventos de administración de lectura y escritura](#)

- [\[CloudTrail.6\] Asegúrese de que el depósito de S3 que se utiliza para almacenar CloudTrail los registros no sea de acceso público](#)
- [\[CloudWatch.15\] Las alarmas de CloudWatch deben tener configuradas acciones específicas](#)
- [\[CloudWatch.16\] Los grupos de registros de CloudWatch deben retenerse durante un periodo específico](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[CodeBuild.1\] CodeBuild El repositorio fuente de Bitbucket no URLs debe contener credenciales confidenciales](#)
- [\[CodeBuild.7\] las exportaciones de grupos de CodeBuild informes deben cifrarse en reposo](#)
- [\[Cognito.1\] 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](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.1\] Las instancias de replicación de Database Migration Service no deben ser públicas](#)
- [\[DMS.2\] DMS los certificados deben estar etiquetados](#)
- [\[DMS.3\] las suscripciones a DMS eventos deben estar etiquetadas](#)
- [\[DMS.4\] las instancias de DMS replicación deben estar etiquetadas](#)
- [\[DMS.5\] los grupos de subredes de DMS replicación deben estar etiquetados](#)
- [\[DMS.6\] las instancias de DMS replicación deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] las tareas de DMS replicación de la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] las tareas de DMS replicación de la base de datos de origen deben tener el registro activado](#)
- [\[DMS.9\] Los DMS puntos finales deben utilizar SSL](#)
- [\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización IAM](#)
- [\[DMS.11\] DMS Los puntos finales de MongoDB deberían tener habilitado un mecanismo de autenticación](#)
- [\[DMS.12\] DMS Los puntos finales de Redis deberían estar habilitados OSS TLS](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.4\] 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](#)
- [\[EC2.3\] Los volúmenes adjuntos de Amazon EBS deben cifrarse en reposo](#)
- [\[EC2.4\] EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico](#)
- [\[EC2.6\] El registro de flujo de VPC debe estar habilitado en todas VPCs](#)
- [\[EC2.8\] EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancias IMDSv2](#)
- [\[EC2.12\] Amazon no utilizado EC2 EIPs debería retirarse](#)
- [\[EC2.13\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 22](#)
- [\[EC2.14\] Los grupos de seguridad no deberían permitir la entrada desde el 0.0.0.0/0 o: :/0 al puerto 3389](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon no utilizados deberían eliminarse](#)
- [\[EC2.24\] No se deben usar 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 respaldo](#)
- [\[EC2.51\] Los puntos finales de 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 utilizar la versión 2 \(\) del Servicio de Metadatos de Instancia IMDSv2](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[ECS.1\] Las definiciones de ECS tareas de Amazon deben tener modos de red seguros y definiciones de usuario.](#)
- [\[ECS.9\] las definiciones de ECS tareas deben tener una configuración de registro](#)
- [\[EFS.1\] El sistema de archivos elástico debe configurarse para cifrar los datos de los archivos en reposo mediante AWS KMS](#)
- [\[EFS.2\] EFS Los volúmenes de Amazon deberían estar en los planes de respaldo](#)

- [\[ELB.1\] Application Load Balancer debe configurarse para redirigir todas las HTTP solicitudes a HTTPS](#)
- [\[ELB.3\] Los oyentes de Classic Load Balancer deben configurarse con o con terminación HTTPS TLS](#)
- [\[ELB.9\] Los balanceadores de carga clásicos deberían tener activado el balanceo de cargas entre zonas](#)
- [\[ELB.14\] El Classic Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.16\] Los balanceadores de carga de aplicaciones deben estar asociados a una web AWS WAF ACL](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(RedisOSS\) 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 \(RedisOSS\) de versiones anteriores deberían tener Redis activado OSS AUTH](#)
- [\[ElastiCache.7\] 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](#)
- [\[EventBridge.3\] 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](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[GuardDuty.2\] GuardDuty los filtros deben estar etiquetados](#)

- [\[GuardDuty.9\] La GuardDuty RDS protección 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](#)
- [\[IAM.8\] Deben eliminarse las credenciales de usuario de IAM no utilizadas](#)
- [\[IAM.9\] La MFA debe estar habilitada para el usuario raíz](#)
- [\[IAM.18\] Asegúrese de que se haya creado una función de soporte para gestionar los incidentes con Soporte](#)
- [\[IAM.19\] 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 la política adjunta AWSCloud ShellFullAccess](#)
- [\[Inspector.1\] El EC2 escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.2\] El ECR escaneo de Amazon Inspector debe estar activado](#)
- [\[Inspector.3\] 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](#)
- [\[KMS.1\] 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 MSK Connect deben estar cifrados 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](#)
- [\[RDS.1\] 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 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](#)
- [Las instancias RDS \[RDS.11\] deben tener habilitadas las copias de seguridad automáticas](#)
- [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 clústeres de Redshift \[Redshift.9\] no deben usar el nombre de base de datos predeterminado](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.2\] 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](#)
- [\[S3.5\] Los depósitos de uso general de S3 deberían requerir solicitudes de uso SSL](#)
- [\[S3.6\] Las políticas de compartimentos de uso general de S3 deberían restringir el acceso a otras Cuentas de AWS](#)
- [\[S3.14\] Los buckets de uso general de S3 deben tener habilitado el control de versiones](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[SageMaker.1\] Las instancias de Amazon SageMaker AI notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] Las instancias de SageMaker AI notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker AI Notebook](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [\[SNS.1\] SNS los temas deben cifrarse en reposo mediante AWS KMS](#)
- [Las colas de Amazon SQS \[SQS.1\] deben cifrarse en reposo](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SSM.1\] EC2 Las instancias de Amazon deben gestionarse mediante AWS Systems Manager](#)
- [\[StepFunctions.1\] Las máquinas de estado de Step Functions deberían tener el registro activado](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.3\] Los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)

- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.10\] la AWS WAF web ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)
- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

América del Sur (São Paulo)

Los siguientes controles no se admiten en América del Sur (São Paulo).

- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[GlobalAccelerator.1\] Los aceleradores de Global Accelerator deben etiquetarse](#)
- [\[IAM.26\] Los certificados SSL/TLS vencidos administrados en IAM deben eliminarse](#)
- [\[Inspector.3\] El análisis de código de Lambda en Amazon Inspector debe estar habilitado](#)

- [\[IoT.1\] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse](#)
- [\[IoT.2\] Las acciones de mitigación de AWS IoT Core deben etiquetarse](#)
- [\[IoT.3\] Las dimensiones de AWS IoT Core deben etiquetarse](#)
- [Los clústeres de RDS \[RDS.7\] deben tener habilitada la protección contra la eliminación](#)
- [La autenticación de IAM \[RDS.12\] debe configurarse para los clústeres de RDS](#)
- [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](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.24\] Los puntos de acceso de varias regiones de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)

AWS GovCloud (EEUU-Este)

Los siguientes controles no se admiten en AWS GovCloud (EE. UU. Este).

- [\[ACM.2\] RSA los certificados gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)
- [\[ACM.3\] ACM los certificados deben estar etiquetados](#)
- [\[Account.1\] La información de contacto de seguridad debe proporcionarse para una Cuenta de AWS](#)
- [\[Account.2\] Cuentas de AWS debe ser parte de una organización de AWS Organizations](#)
- [\[APIGateway.2\] REST API Las etapas de la API puerta de enlace deben configurarse para usar SSL certificados para la autenticación de fondo](#)
- [\[APIGateway.3\] REST API Las etapas de API Gateway deben tener habilitado el AWS X-Ray rastreo](#)
- [\[APIGateway.4\] La API puerta de enlace debe estar asociada a una web WAF ACL](#)

- [\[APIGateway.8\] Las rutas de API gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas de API Gateway V2](#)
- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.2\] AWS AppSync debe tener activado 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 API](#)
- [\[AppSync.6\] AWS AppSync API Las cachés 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](#)
- [\[AutoScaling.2\] 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](#)
- [\[AutoScaling.5\] EC2 Las instancias de Amazon lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas](#)
- [\[Backup.2\] Los puntos de recuperación de AWS Backup deben etiquetarse](#)
- [\[Backup.3\] Los almacenes de AWS Backup deben etiquetarse](#)
- [\[Backup.4\] Los planes de informes de AWS Backup deben etiquetarse](#)
- [\[Backup.5\] Los planes de copias de seguridad de AWS Backup deben etiquetarse](#)
- [\[CloudFormation.2\] Las pilas de CloudFormation deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)

- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CloudTrail.9\] las CloudTrail rutas deben estar etiquetadas](#)
- [\[CloudWatch.15\] Las alarmas de CloudWatch deben tener configuradas acciones específicas](#)
- [\[CloudWatch.16\] Los grupos de registros de CloudWatch deben retenerse durante un periodo específico](#)
- [\[CloudWatch.17\] Las acciones de alarma de CloudWatch deben estar activadas](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[CodeBuild.1\] 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](#)
- [\[Cognito.1\] 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](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.2\] DMS los certificados deben estar etiquetados](#)
- [\[DMS.3\] las suscripciones a DMS eventos deben estar etiquetadas](#)
- [\[DMS.4\] las instancias de DMS replicación deben estar etiquetadas](#)
- [\[DMS.5\] los grupos de subredes de DMS replicación deben estar etiquetados](#)
- [\[DMS.6\] las instancias de DMS replicación deben tener habilitada la actualización automática de las versiones secundarias](#)

- [\[DMS.7\] las tareas de DMS replicación de la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] las tareas de DMS replicación de la base de datos de origen deben tener el registro activado](#)
- [\[DMS.9\] Los DMS puntos finales deben utilizar 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](#)
- [\[DynamoDB.1\] Las tablas de DynamoDB deberían escalar automáticamente la capacidad en función de la demanda](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.5\] Las tablas de DynamoDB deben etiquetarse](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.15\] EC2 Las subredes de Amazon no deberían 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](#)
- [\[EC2.21\] La red no ACLs debe permitir la entrada desde el 0.0.0.0/0 al puerto 22 o al puerto 3389](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon no utilizados deberían eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC2.24\] No se deben usar 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 respaldo](#)

- [\[EC2.33\] Los archivos adjuntos a las pasarelas de EC2 tránsito deben estar etiquetados](#)
- [\[EC2.34\] Las tablas de rutas de las pasarelas de EC2 tránsito deben estar etiquetadas](#)
- [Las interfaces de EC2 red deben estar etiquetadas \[EC2.35\]](#)
- [\[EC2.36\] Las pasarelas de EC2 clientes deben estar etiquetadas](#)
- [\[EC2.37\] Las direcciones IP EC2 elásticas deben estar etiquetadas](#)
- [\[EC2.38\] EC2 las instancias deben estar etiquetadas](#)
- [\[EC2.39\] Las pasarelas EC2 de Internet deben estar etiquetadas](#)
- [\[EC2.40\] Las pasarelas EC2 NAT deben estar etiquetadas](#)
- [La EC2 red \[EC2.41\] ACLs debe estar etiquetada](#)
- [Las tablas de EC2 rutas deben estar etiquetadas \[EC2.42\]](#)
- [\[EC2.43\] 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 punto final de Amazon VPC deben estar etiquetados](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben estar etiquetados](#)
- [\[EC2.49\] Las conexiones de emparejamiento de Amazon VPC deben estar etiquetadas](#)
- [\[EC2.50\] Las pasarelas de EC2 VPN deben estar etiquetadas](#)
- [\[EC2.52\] Las pasarelas de EC2 tránsito 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 utilizar la versión 2 \(\) del Servicio de Metadatos de Instancia IMDSv2](#)
- [\[ECR.1\] Los repositorios ECR privados deben tener configurado el escaneo de imágenes](#)
- [\[ECR.2\] Los repositorios ECR privados deben tener configurada la inmutabilidad de las etiquetas](#)
- [\[ECR.3\] ECR Los repositorios deben tener configurada al menos una política de ciclo de vida](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[ECS.1\] Las definiciones de ECS tareas de Amazon deben tener modos de red seguros y definiciones de usuario.](#)

- [\[ECS.3\] las definiciones de ECS tareas no deben compartir el espacio de nombres del proceso del host](#)
- [\[ECS.4\] los ECS contenedores deberían ejecutarse sin privilegios](#)
- [\[ECS.5\] ECS Los contenedores 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 ECS tareas deben tener una configuración de registro](#)
- [\[ECS.10\] Los servicios de ECS Fargate deberían ejecutarse en la última versión de la plataforma Fargate](#)
- [\[ECS.12\] ECS los clústeres deben usar Container Insights](#)
- [\[ECS.13\] ECS los servicios deben estar etiquetados](#)
- [\[ECS.14\] los ECS clústeres deben estar etiquetados](#)
- [\[ECS.15\] Las definiciones de ECS tareas deben estar etiquetadas](#)
- [\[EFS.2\] EFS Los volúmenes de Amazon deberían estar en los planes de respaldo](#)
- [\[EFS.3\] los puntos de EFS acceso deben establecer un directorio raíz](#)
- [\[EFS.4\] los puntos de EFS acceso deben imponer la identidad de un usuario](#)
- [\[EFS.5\] los puntos de EFS acceso deben estar etiquetados](#)
- [\[EKS.1\] Los puntos finales de los EKS clústeres no deben ser de acceso público](#)
- [\[EKS.2\] EKS los clústeres deberían ejecutarse en una versión compatible de Kubernetes](#)
- [\[EKS.6\] EKS los clústeres deben estar etiquetados](#)
- [\[EKS.7\] Las configuraciones de los proveedores de EKS identidad deben estar etiquetadas](#)
- [\[EKS.8\] EKS los clústeres deben tener habilitado el registro de auditoría](#)
- [\[ELB.2\] Los balanceadores de carga clásicos con HTTPS listenersSSL/deben usar un certificado proporcionado por AWS Certificate Manager](#)
- [\[ELB.8\] Los balanceadores de carga clásicos que utilizan dispositivos de SSL escucha deben usar una política de seguridad predefinida que tenga una larga duración AWS Config](#)
- [\[ELB.10\] Classic Load Balancer debe abarcar varias zonas de disponibilidad](#)
- [\[ELB.12\] Application Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.13\] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad](#)

- [\[ELB.14\] El Classic Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.16\] Los balanceadores de carga de aplicaciones deben estar asociados a una web AWS WAF ACL](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(RedisOSS\) 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 \(RedisOSS\) de versiones anteriores deberían tener Redis activado OSS AUTH](#)
- [\[ElastiCache.7\] 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](#)
- [\[ES.4\] 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](#)
- [\[FSx.1\] FSx para sistemas de ZFS archivos abiertos, debe configurarse para copiar etiquetas a 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 etiquetarse](#)
- [\[Glue.1\] los AWS Glue trabajos deben estar etiquetados](#)
- [\[Glue.3\] Las transformaciones AWS Glue de aprendizaje automático deben cifrarse en reposo](#)
- [\[GuardDuty.1\] GuardDuty debe 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](#)
- [\[GuardDuty.7\] La monitorización del GuardDuty EKS tiempo de ejecución debe estar habilitada](#)
- [\[GuardDuty.8\] La protección contra GuardDuty malware para EC2 debe estar habilitada](#)
- [\[GuardDuty.9\] La GuardDuty RDS protección 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](#)
- [\[IAM.28\] 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](#)
- [\[IoT.1\] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse](#)
- [\[IoT.2\] Las acciones de mitigación de AWS IoT Core deben etiquetarse](#)
- [\[IoT.3\] Las dimensiones de AWS IoT Core deben etiquetarse](#)
- [\[IoT.4\] Los autorizadores de AWS IoT Core deben etiquetarse](#)
- [\[IoT.5\] Los alias de los roles de AWS IoT Core deben etiquetarse](#)
- [\[IoT.6\] Las políticas de AWS IoT Core deben etiquetarse](#)
- [\[Kinesis.1\] Las transmisiones de Kinesis deben cifrarse en reposo](#)
- [\[Kinesis.2\] Las transmisiones de Kinesis deben etiquetarse](#)
- [\[KMS.5\] Las claves KMS no deben ser de acceso público](#)
- [\[Lambda.5\] Las funciones VPC Lambda 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](#)
- [\[MQ.3\] 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](#)
- [\[MSK.1\] MSK Los clústeres deben cifrarse en tránsito entre los nodos intermediarios](#)
- [\[MSK.2\] MSK los clústeres deben tener configurada una supervisión mejorada](#)
- [\[MSK.3\] Los conectores MSK Connect deben estar cifrados 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 bases de datos de Neptune deben tener habilitada la autenticación de bases de datos 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](#)
- [\[NetworkFirewall.1\] Los 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](#)
- [\[NetworkFirewall.7\] Los firewall de Network Firewall se deben etiquetar](#)
- [\[NetworkFirewall.8\] Las políticas de firewall de Network Firewall se deben etiquetar](#)
- [Los firewalls de Network Firewall \[NetworkFirewall.9\] 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](#)
- [Los OpenSearch dominios \[Opensearch.9\] deben estar etiquetados](#)
- [La autoridad emisora de certificados AWS Private CA raíz \[PCA.1\] debe estar deshabilitada](#)
- [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](#)

- [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](#)
- [\[Redshift.7\] Los clústeres de Redshift deberían utilizar un enrutamiento mejorado VPC](#)
- [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](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.1\] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[S3.8\] Los buckets de uso general de S3 deben bloquear el acceso público](#)
- [\[S3.10\] 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](#)

- [\[S3.20\] Los cubos de uso general de S3 deberían tener habilitada la función de eliminación 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 AI notebook no deberían tener acceso directo a Internet](#)
- [\[SageMaker.2\] Las instancias de SageMaker AI notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker AI Notebook](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [\[SecretsManager.3\] 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](#)
- [\[SNS.3\] SNS los temas deben estar etiquetados](#)
- [\[SNS.4\] las políticas de acceso a los SNS temas no deberían permitir el acceso público](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SSM.4\] SSM los documentos no deben ser públicos](#)
- [\[StepFunctions.1\] Las máquinas de estado de Step Functions deberían tener el registro activado](#)
- [\[StepFunctions.2\] Las actividades de Step Functions deben estar etiquetadas](#)
- [\[Transfer.1\] AWS Transfer Family Los flujos de trabajo deben estar etiquetados](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.2\] Las reglas regionales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.3\] Los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.4\] La web regional AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.10\] la AWS WAF web ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado](#)

- [\[WAF.12\] AWS WAF las reglas deben tener las CloudWatch métricas habilitadas](#)
- [\[WorkSpaces.1\] Los volúmenes de usuarios de WorkSpaces deben estar cifrados en reposo](#)
- [\[WorkSpaces.2\] Los volúmenes raíz de WorkSpaces deben estar cifrados en reposo](#)

AWS GovCloud (EEUU-Oeste)

Los siguientes controles no se admiten en AWS GovCloud (EE. UU. y oeste).

- [\[ACM.2\] RSA los certificados gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits](#)
- [\[ACM.3\] ACM los certificados deben estar etiquetados](#)
- [\[Account.1\] La información de contacto de seguridad debe proporcionarse para una Cuenta de AWS](#)
- [\[Account.2\] Cuentas de AWS debe ser parte de una organización de AWS Organizations](#)
- [\[APIGateway.2\] REST API Las etapas de la API puerta de enlace deben configurarse para usar SSL certificados para la autenticación de fondo](#)
- [\[APIGateway.3\] REST API Las etapas de API Gateway deben tener habilitado el AWS X-Ray rastreo](#)
- [\[APIGateway.4\] La API puerta de enlace debe estar asociada a una web WAF ACL](#)
- [\[APIGateway.8\] Las rutas de API gateway deben especificar un tipo de autorización](#)
- [\[APIGateway.9\] El registro de acceso debe configurarse para las etapas de API Gateway V2](#)
- [\[AppSync.1\] las AWS AppSync API cachés deben cifrarse en reposo](#)
- [\[AppSync.2\] AWS AppSync debe tener activado 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 API](#)
- [\[AppSync.6\] AWS AppSync API Las cachés 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](#)
- [\[AutoScaling.2\] 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](#)
- [\[AutoScaling.5\] EC2 Las instancias de Amazon lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas](#)
- [\[Backup.2\] Los puntos de recuperación de AWS Backup deben etiquetarse](#)
- [\[Backup.3\] Los almacenes de AWS Backup deben etiquetarse](#)
- [\[Backup.4\] Los planes de informes de AWS Backup deben etiquetarse](#)
- [\[Backup.5\] Los planes de copias de seguridad de AWS Backup deben etiquetarse](#)
- [\[CloudFormation.2\] Las pilas de CloudFormation deben etiquetarse](#)
- [\[CloudFront.1\] CloudFront las distribuciones deben tener configurado un objeto raíz predeterminado](#)
- [\[CloudFront.3\] CloudFront las distribuciones deberían requerir el cifrado en tránsito](#)
- [\[CloudFront.4\] CloudFront las distribuciones deben tener configurada la conmutación por error de Origin](#)
- [\[CloudFront.5\] CloudFront las distribuciones deberían tener el registro activado](#)
- [\[CloudFront.6\] CloudFront las distribuciones deberían estar habilitadas WAF](#)
- [\[CloudFront.7\] CloudFront las distribuciones deben usar certificados/personalizados SSL TLS](#)
- [\[CloudFront.8\] CloudFront las distribuciones deberían usarse SNI para atender las solicitudes HTTPS](#)
- [\[CloudFront.9\] CloudFront las distribuciones deberían cifrar el tráfico hacia orígenes personalizados](#)
- [\[CloudFront.10\] CloudFront las distribuciones no deberían usar SSL protocolos obsoletos entre las ubicaciones de los bordes 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 al origen](#)
- [\[CloudFront.14\] CloudFront las distribuciones deben estar etiquetadas](#)
- [\[CloudTrail.9\] las CloudTrail rutas deben estar etiquetadas](#)
- [\[CloudWatch.15\] Las alarmas de CloudWatch deben tener configuradas acciones específicas](#)

- [\[CloudWatch.16\] Los grupos de registros de CloudWatch deben retenerse durante un periodo específico](#)
- [\[CloudWatch.17\] Las acciones de alarma de CloudWatch deben estar activadas](#)
- [\[CodeArtifact.1\] Los repositorios de CodeArtifact deben etiquetarse](#)
- [\[CodeBuild.1\] 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](#)
- [\[Cognito.1\] 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](#)
- [\[Detective.1\] Los gráficos de comportamiento de Detective deben estar etiquetados](#)
- [\[DMS.2\] DMS los certificados deben estar etiquetados](#)
- [\[DMS.3\] las suscripciones a DMS eventos deben estar etiquetadas](#)
- [\[DMS.4\] las instancias de DMS replicación deben estar etiquetadas](#)
- [\[DMS.5\] los grupos de subredes de DMS replicación deben estar etiquetados](#)
- [\[DMS.6\] las instancias de DMS replicación deben tener habilitada la actualización automática de las versiones secundarias](#)
- [\[DMS.7\] las tareas de DMS replicación de la base de datos de destino deben tener habilitado el registro](#)
- [\[DMS.8\] las tareas de DMS replicación de la base de datos de origen deben tener el registro activado](#)
- [\[DMS.9\] Los DMS puntos finales deben utilizar 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](#)
- [\[DynamoDB.1\] Las tablas de DynamoDB deberían escalar automáticamente la capacidad en función de la demanda](#)
- [\[DynamoDB.3\] Los clústeres de DynamoDB Accelerator \(\) deben cifrarse en reposo DAX](#)
- [\[DynamoDB.4\] Las tablas de DynamoDB deben estar presentes en un plan de copias de seguridad](#)
- [\[DynamoDB.5\] Las tablas de DynamoDB deben etiquetarse](#)
- [\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito](#)
- [\[EC2.15\] EC2 Las subredes de Amazon no deberían 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](#)
- [\[EC2.21\] La red no ACLs debe permitir la entrada desde el 0.0.0.0/0 al puerto 22 o al puerto 3389](#)
- [\[EC2.22\] Los grupos de EC2 seguridad de Amazon no utilizados deberían eliminarse](#)
- [\[EC2.23\] Amazon EC2 Transit Gateways no debe aceptar automáticamente las solicitudes de adjuntos de VPC](#)
- [\[EC2.24\] No se deben usar 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 respaldo](#)
- [\[EC2.33\] Los archivos adjuntos a las pasarelas de EC2 tránsito deben estar etiquetados](#)
- [\[EC2.34\] Las tablas de rutas de las pasarelas de EC2 tránsito deben estar etiquetadas](#)
- [Las interfaces de EC2 red deben estar etiquetadas \[EC2.35\]](#)
- [\[EC2.36\] Las pasarelas de EC2 clientes deben estar etiquetadas](#)
- [\[EC2.37\] Las direcciones IP EC2 elásticas deben estar etiquetadas](#)
- [\[EC2.38\] EC2 las instancias deben estar etiquetadas](#)
- [\[EC2.39\] Las pasarelas EC2 de Internet deben estar etiquetadas](#)
- [\[EC2.40\] Las pasarelas EC2 NAT deben estar etiquetadas](#)
- [La EC2 red \[EC2.41\] ACLs debe estar etiquetada](#)
- [Las tablas de EC2 rutas deben estar etiquetadas \[EC2.42\]](#)
- [\[EC2.43\] 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 punto final de Amazon VPC deben estar etiquetados](#)
- [\[EC2.48\] Los registros de flujo de Amazon VPC deben estar etiquetados](#)
- [\[EC2.49\] Las conexiones de emparejamiento de Amazon VPC deben estar etiquetadas](#)
- [\[EC2.50\] Las pasarelas de EC2 VPN deben estar etiquetadas](#)
- [\[EC2.52\] Las pasarelas de EC2 tránsito 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 utilizar la versión 2 \(\) del Servicio de Metadatos de Instancia IMDSv2](#)
- [\[ECR.1\] Los repositorios ECR privados deben tener configurado el escaneo de imágenes](#)
- [\[ECR.2\] Los repositorios ECR privados deben tener configurada la inmutabilidad de las etiquetas](#)
- [\[ECR.3\] ECR Los repositorios deben tener configurada al menos una política de ciclo de vida](#)
- [\[ECR.4\] Los repositorios ECR públicos deben estar etiquetados](#)
- [\[ECS.1\] Las definiciones de ECS tareas de Amazon deben tener modos de red seguros y definiciones de usuario.](#)
- [\[ECS.3\] las definiciones de ECS tareas no deben compartir el espacio de nombres del proceso del host](#)
- [\[ECS.4\] los ECS contenedores deberían ejecutarse sin privilegios](#)
- [\[ECS.5\] ECS Los contenedores 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 ECS tareas deben tener una configuración de registro](#)
- [\[ECS.10\] Los servicios de ECS Fargate deberían ejecutarse en la última versión de la plataforma Fargate](#)
- [\[ECS.12\] ECS los clústeres deben usar Container Insights](#)
- [\[ECS.13\] ECS los servicios deben estar etiquetados](#)
- [\[ECS.14\] los ECS clústeres deben estar etiquetados](#)

- [\[ECS.15\] Las definiciones de ECS tareas deben estar etiquetadas](#)
- [\[EFS.2\] EFS Los volúmenes de Amazon deberían estar en los planes de respaldo](#)
- [\[EFS.3\] los puntos de EFS acceso deben establecer un directorio raíz](#)
- [\[EFS.4\] los puntos de EFS acceso deben imponer la identidad de un usuario](#)
- [\[EFS.5\] los puntos de EFS acceso deben estar etiquetados](#)
- [\[EKS.1\] Los puntos finales de los EKS clústeres no deben ser de acceso público](#)
- [\[EKS.2\] EKS los clústeres deberían ejecutarse en una versión compatible de Kubernetes](#)
- [\[EKS.6\] EKS los clústeres deben estar etiquetados](#)
- [\[EKS.7\] Las configuraciones de los proveedores de EKS identidad deben estar etiquetadas](#)
- [\[EKS.8\] EKS los clústeres deben tener habilitado el registro de auditoría](#)
- [\[ELB.10\] Classic Load Balancer debe abarcar varias zonas de disponibilidad](#)
- [\[ELB.12\] Application Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.13\] Los balanceadores de carga de aplicaciones, redes y puertas de enlace deben abarcar varias zonas de disponibilidad](#)
- [\[ELB.14\] El Classic Load Balancer debe configurarse con el modo defensivo o de mitigación de desincronización más estricto](#)
- [\[ELB.16\] Los balanceadores de carga de aplicaciones deben estar asociados a una web AWS WAF ACL](#)
- [\[ElastiCache.1\] Los clústeres ElastiCache \(RedisOSS\) 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 \(RedisOSS\) de versiones anteriores deberían tener Redis activado OSS AUTH](#)
- [\[ElastiCache.7\] 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](#)
- [\[ES.4\] 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](#)
- [\[FSx.1\] FSx para sistemas de ZFS archivos abiertos, debe configurarse para copiar etiquetas a 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 etiquetarse](#)
- [\[Glue.1\] 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](#)
- [\[GuardDuty.7\] La monitorización del GuardDuty EKS tiempo de ejecución debe estar habilitada](#)
- [\[GuardDuty.8\] La protección contra GuardDuty malware para EC2 debe estar habilitada](#)
- [\[GuardDuty.9\] La GuardDuty RDS protección 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](#)
- [\[IAM.28\] 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](#)
- [\[IoT.1\] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse](#)
- [\[IoT.2\] Las acciones de mitigación de AWS IoT Core deben etiquetarse](#)
- [\[IoT.3\] Las dimensiones de AWS IoT Core deben etiquetarse](#)
- [\[IoT.4\] Los autorizadores de AWS IoT Core deben etiquetarse](#)
- [\[IoT.5\] Los alias de los roles de AWS IoT Core deben etiquetarse](#)
- [\[IoT.6\] Las políticas de AWS IoT Core deben etiquetarse](#)
- [\[Kinesis.1\] Las transmisiones de Kinesis deben cifrarse en reposo](#)
- [\[Kinesis.2\] Las transmisiones de Kinesis deben etiquetarse](#)
- [\[KMS.5\] Las claves KMS no deben ser de acceso público](#)
- [\[Lambda.5\] Las funciones VPC Lambda 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](#)
- [\[MQ.3\] 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](#)
- [\[MSK.1\] MSK Los clústeres deben cifrarse en tránsito entre los nodos intermediarios](#)
- [\[MSK.2\] MSK los clústeres deben tener configurada una supervisión mejorada](#)
- [\[MSK.3\] Los conectores MSK Connect deben estar cifrados 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 bases de datos de Neptune deben tener habilitada la autenticación de bases de datos 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](#)
- [\[NetworkFirewall.1\] Los 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](#)
- [\[NetworkFirewall.7\] Los firewall de Network Firewall se deben etiquetar](#)
- [\[NetworkFirewall.8\] Las políticas de firewall de Network Firewall se deben etiquetar](#)
- [Los firewalls de Network Firewall \[NetworkFirewall.9\] 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](#)
- [Los OpenSearch dominios \[Opensearch.9\] deben estar etiquetados](#)
- [La autoridad emisora de certificados AWS Private CA raíz \[PCA.1\] debe estar deshabilitada](#)

- [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](#)
- [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](#)
- [\[Redshift.7\] Los clústeres de Redshift deberían utilizar un enrutamiento mejorado VPC](#)
- [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](#)
- [\[Route53.1\] Las comprobaciones de estado de Route 53 deben estar etiquetadas](#)
- [\[Route53.2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS](#)
- [\[S3.1\] Los buckets de uso general de S3 deben tener habilitado el bloqueo de acceso público](#)
- [\[S3.8\] Los buckets de uso general de S3 deben bloquear el acceso público](#)
- [\[S3.10\] 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](#)
- [\[S3.20\] Los cubos de uso general de S3 deberían tener habilitada la función de eliminación 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 AI notebook deben lanzarse en una VPC personalizada](#)
- [\[SageMaker.3\] Los usuarios no deberían tener acceso root a las instancias de SageMaker AI Notebook](#)
- [\[SES.1\] Las listas de contactos de SES deben estar etiquetadas](#)
- [\[SES.2\] Los conjuntos de configuración de SES deben estar etiquetados](#)
- [\[SecretsManager.3\] 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](#)
- [\[SNS.3\] SNS los temas deben estar etiquetados](#)
- [\[SNS.4\] las políticas de acceso a los SNS temas no deberían permitir el acceso público](#)
- [\[SQS.2\] Las colas de SQS deben estar etiquetadas](#)
- [\[SSM.4\] SSM los documentos no deben ser públicos](#)
- [\[StepFunctions.1\] Las máquinas de estado de Step Functions deberían tener el registro activado](#)
- [\[StepFunctions.2\] Las actividades de Step Functions deben estar etiquetadas](#)

- [\[Transfer.1\] AWS Transfer Family Los flujos de trabajo deben estar etiquetados](#)
- [\[WAF.1\] AWS WAF El ACL registro web global clásico debe estar habilitado](#)
- [\[WAF.2\] Las reglas regionales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.3\] Los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.4\] La web regional AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.6\] Las reglas globales AWS WAF clásicas deben tener al menos una condición](#)
- [\[WAF.7\] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla](#)
- [\[WAF.8\] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.10\] la AWS WAF web ACLs debe tener al menos una regla o grupo de reglas](#)
- [\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado](#)
- [\[WAF.12\] AWS WAF las reglas deben tener las CloudWatch métricas habilitadas](#)

Deshabilitación de Security Hub

Note

Si utilizas la configuración central, el administrador delegado del AWS Security Hub puede crear políticas de configuración que inhabiliten Security Hub en cuentas y unidades organizativas específicas (OUs) y lo mantengan activado en otras. Las políticas de configuración entran en vigor en la región de origen y en todas las regiones vinculadas. Para obtener más información, consulte [Comprensión de la configuración centralizada en Security Hub](#).

Puede usar la consola de Security Hub, Security Hub API o AWS CLI deshabilitar Security Hub.

Cuando deshabilita Security Hub en una cuenta, ocurre lo siguiente:

- No se generan ni ingieren nuevos hallazgos para la cuenta.
- Transcurridos 90 días, sus resultados e informaciones existentes y cualquier ajuste de configuración de Security Hub se eliminan de forma irrecuperable.

Si desea guardar sus resultados actuales, debe exportarlos antes de deshabilitar Security Hub. Para obtener más información, consulte [the section called “Efecto de las acciones de la cuenta en los datos de Security Hub”](#).

- Cualquier estándar y control habilitado se deshabilita.

No puede deshabilitar Security Hub en los siguientes casos:

- Su cuenta es la cuenta de administrador de Security Hub designada para una organización. Si utiliza la configuración centralizada, no puede asociar una política de configuración que deshabilite Security Hub con la cuenta de administrador delegado. La asociación puede funcionar correctamente en otras cuentas, pero Security Hub no aplica dicha política a la cuenta de administrador delegado.
- Su cuenta es una cuenta de administrador de Security Hub por invitación y tiene cuentas miembro. Para poder deshabilitar Security Hub, antes debe desvincular todas sus cuentas miembro. Consulte [the section called “Cómo desvincular las cuentas de miembro en Security Hub”](#).

Para que el propietario de una cuenta miembro pueda desactivar Security Hub, la cuenta no debe estar asociada a su cuenta de administrador. En el caso de una cuenta de organización, solo la cuenta de administrador puede desvincular cuentas miembro. Para obtener más información, consulte [the section called “Desasociación de cuentas de la organización como cuentas de miembro”](#). En el caso de cuentas invitadas manualmente, tanto la cuenta de administrador como la cuenta miembro pueden desvincular la cuenta miembro. Para obtener más información, consulte [the section called “Cómo desvincular las cuentas de miembro en Security Hub”](#) o [the section called “Desvincularse de una cuenta de administrador de Security Hub”](#). La desasociación no es necesaria si utiliza la configuración centralizada, ya que puede crear una política que deshabilite Security Hub en cuentas de miembros específicas.

Al deshabilitar Security Hub en una cuenta, se deshabilita solo en la región actual. Sin embargo, si utiliza la configuración centralizada para deshabilitar Security Hub en cuentas específicas, se deshabilitará en la región de origen y en todas las regiones vinculadas.

Elija el método que prefiera y siga estos pasos para deshabilitar Security Hub.

Security Hub console

Deshabilitación de Security Hub

1. Abra la consola AWS de Security Hub en <https://console.aws.amazon.com/securityhub/>.
2. En el panel de navegación, seleccione Configuración.
3. En la página Configuración, seleccione General.
4. En Disable AWS Security Hub, selecciona Disable AWS Security Hub. A continuación, selecciona Disable AWS Security Hub de nuevo.

Security Hub API

Deshabilitación de Security Hub

Invoca el [DisableSecurityHubAPI](#).

AWS CLI

Deshabilitación de Security Hub

Ejecute el comando [disable-security-hub](#).

Comando de ejemplo:

```
aws securityhub disable-security-hub
```

Registro de cambios en los controles de Security Hub

El siguiente registro de cambios registra los cambios importantes en los controles de AWS Security Hub seguridad existentes, 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 evalúa Security Hub el estado de los controles, consulte [Evaluación del estado de control y el estado de conformidad en Security Hub](#). Los cambios pueden tardar unos días después de su entrada en este registro y afectar a todos los elementos Regiones de AWS en los que esté disponible el control.

Este registro realiza el seguimiento de los cambios que se han producido desde abril de 2023.

Seleccione un control para ver más detalles al respecto. Los cambios de título se indican en la descripción detallada de cada control durante 90 días.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de enero de 2025	[Glue.2] Los trabajos de AWS pegado deberían tener habilitado el registro	Security Hub ha retirado este control y lo ha eliminado de todos los estándares.
20 de diciembre de 2024	EC26.1 a 1.69 EC2	Security Hub revirtió la versión de EC2 6.1 a EC2 1.69.
12 de diciembre de 2024	Las instancias RDS [RDS.23] no deben usar el puerto predeterminado de un motor de base de datos	RDS.23 comprueba si un clúster o instancia de Amazon Relational Database Service (RDSAmazon) utiliza un puerto distinto del puerto predeterminado del motor de base de datos. Hemos actualizado el control para que

Fecha del cambio	ID y título de control	Descripción del cambio
		<p>la AWS Config regla subyacente devuelva un resultado de NOT_APPLICABLE las RDS instancias que forman parte de un clúster.</p>
<p>2 de diciembre de 2024</p>	<p>[Lambda.2] Las funciones de Lambda deben usar los tiempos de ejecución admitidos</p>	<p>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. Ahora Security Hub admite <code>nodejs22.x</code> como parámetro.</p>
<p>26 de noviembre de 2024</p>	<p>[EKS.2] EKS los clústeres deberían ejecutarse en una versión compatible de Kubernetes</p>	<p>Este control comprueba si un clúster de Amazon Elastic Kubernetes Service (EKSAmazon) se ejecuta en una versión de Kubernetes compatible. La versión compatible más antigua es 1.29.</p>

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	<p>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 aumentó la severidad de este control de MEDIUM a CRITICAL. Security Hub 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 del Security Hub. Si tiene AWS Config deshabilitado el registro de recursos, puede recibir resultados de control inexactos.</p> <p>Para recibir información sobre Config.1, active el registro de recursos para</p>

Fecha del cambio	ID y título de control	Descripción del cambio
		<p>los recursos que correspondan a los controles de Security Hub habilitados y deshabilite los controles que no sean necesarios en su organización. PASSED Para obtener instrucciones sobre la configuración AWS Config de Security Hub, consulte Activación y configuración AWS Config de Security Hub. Para obtener una lista de los controles de Security Hub y sus recursos correspondientes, consulte AWS Config Recursos necesarios para las conclusiones sobre el control de Security Hub.</p>

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. Ahora Security Hub 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 a 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] Application Load Balancer 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 la DMS .12 y de la ElastiCache .1 a ElastiCache la .7. Hemos cambiado estos títulos para reflejar un cambio de nombre en el servicio Amazon ElastiCache (RedisOSS).

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 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	[IoT.1] Los perfiles de seguridad de AWS IoT Device Defender deben etiquetarse	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 ha dejado de admitir <code>nodejs16.x</code> como parámetro.
29 de julio de 2024	[EKS.2] EKS los clústeres deberían ejecutarse en una versión compatible de Kubernetes	Este control comprueba si un clúster de Amazon Elastic Kubernetes Service (EKSAmazon) 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, utiliza el rol vinculado al servicio y registra los recursos de los controles habilitados. Security Hub actualizó el título del control para reflejar lo que este evalúa.
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 Amazon Aurora My SQL DB está configurado para publicar registros de auditoría en Amazon CloudWatch Logs. Security Hub actualizó el control para que no genere resultados para los clústeres de bases de datos Aurora sin servidor v1.

Fecha del cambio	ID y título de control	Descripción del cambio
11 de junio de 2024	[EKS.2] EKS los clústeres deberían ejecutarse en una versión compatible de Kubernetes	Este control comprueba si un clúster de Amazon Elastic Kubernetes Service (EKSAzón) 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	<p>Este control comprueba si AWS Config está activado y AWS Config el registro de recursos está activado.</p> <p>Anteriormente, el control solo generaba un resultado PASSED si se configuraba el registro para todos los recursos. Security Hub actualizó el control para generar un resultado PASSED cuando se activa el registro 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.</p>

Fecha del cambio	ID y título de control	Descripción del cambio
8 de mayo de 2024	[S3.20] Los cubos de uso general de S3 deberían tener habilitada la función de eliminación MFA	<p>Este control comprueba si un bucket versionado o de uso general de Amazon S3 tiene habilitada la autenticación multifactorial (MFA) delete. Anteriormente, el control generaba un resultado FAILED para los buckets que tenían una configuración de ciclo de vida. Sin embargo, la MFA eliminación con control de versiones no se puede habilitar en un bucket que tenga una configuración de ciclo de vida. Security Hub actualizó el control para no generar resultados para los buckets con una configuración de ciclo de vida. La descripción del control se actualizó para reflejar el comportamiento actual.</p>

Fecha del cambio	ID y título de control	Descripción del cambio
2 de mayo de 2024	[EKS.2] EKS los clústeres deberían ejecutarse en una versión compatible de Kubernetes	Security Hub actualizó la versión compatible e más antigua de Kubernetes en la que se puede ejecutar el EKS clúster de Amazon para producir una conclusión válida. La versión compatible más antigua actual es Kubernetes 1.26.
30 de abril de 2024	[CloudTrail.3] Debe estar habilitada al menos una CloudTrail ruta	Se ha cambiado el título del control de «CloudTrail Debe estar habilitado» a «Al menos una CloudTrail ruta 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 controles de ELB estado	<p>Se ha cambiado el título del control: los grupos de Auto Scaling asociados a un balanceador de cargas clásico deberían usar verificaciones de estado del balanceador de cargas a los grupos de Auto Scaling asociados a un balanceador de cargas deberían usar verificaciones de estado. 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.</p>

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 multirregional que incluya eventos de administración de lectura y escritura	<p>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</p>

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 ha retirado este control y lo ha eliminado 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 ha retirado este control y lo ha eliminado de todos los estándares. Los límites de saltos de respuesta de metadatos para las instancias de Amazon Elastic Compute Cloud (AmazonEC2) 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 Simple Notification Service () SNS	Security Hub ha retirado este control y lo ha eliminado de todos los estándares. Integrar AWS CloudFormation pilas con SNS los temas de Amazon ya no es una práctica recomendada de seguridad. Si bien integrar CloudFormation pilas importantes con SNS temas puede resultar útil, no es obligatorio para todas las pilas.
10 de abril de 2024	[CodeBuild.5] Los entornos de CodeBuild proyectos no deberían tener activado el modo privilegiado	Security Hub ha retirado este control y lo ha eliminado 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] Evite el uso del usuario root	Security Hub ha retirado este control y lo ha eliminado de todos los estándares. El propósito de este control está cubierto por otro control, [CloudWatch.1] Debe existir un filtro de métrica 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 entrega de los mensajes de notificación enviados a un tema	Security Hub ha retirado este control y lo ha eliminado de todos los estándares. Registrar el estado de entrega de SNS los temas ya no es una práctica recomendada de seguridad. Aunque registrar el estado de entrega de SNS los temas importantes 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	<p>Security Hub eliminó este control de AWS Foundational Security Best Practices v1.0.0 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 formando parte de la norma SP 800-53 Rev. 5NIST.</p>

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 eliminó este control de AWS Foundational Security Best Practices v1.0.0 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 formando parte de la norma SP 800-53 Rev. 5NIST.

Fecha del cambio	ID y título de control	Descripción del cambio
10 de abril de 2024	[SNS.1] SNS los temas deben cifrarse en reposo mediante AWS KMS	<p>Security Hub eliminó este control de AWS Foundational Security Best Practices v1.0.0 y Service-Managed Standard: AWS Control Tower De forma predeterminada, SNS cifra los temas en reposo con cifrado de disco. Para más información, consulte Cifrado de datos. Ya no se recomienda su uso AWS KMS para cifrar temas como práctica recomendada de seguridad. Este control sigue formando parte de la norma NIST SP 800-53 Rev. 5.</p>

Fecha del cambio	ID y título de control	Descripción del cambio
8 de abril de 2024	[ELB.6] Los balanceadores de carga de aplicaciones, puertas de enlace y redes deben tener habilitada la protección contra eliminaciones	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	<p>Se cambió el título del control de Las conexiones a OpenSearch los dominios deben cifrarse mediante la versión TLS 1.2 a Las conexiones a OpenSearch los dominios deben cifrarse con la política de TLS seguridad más reciente. Anteriormente, el control solo comprobaba si las conexiones a los OpenSearch dominios utilizaban la TLS versión 1.2. El control ahora determina si los OpenSearch dominios están cifrados con la política de TLS seguridad más reciente. PASSED</p> <p>El título y la descripción del control se actualizaron para reflejar el comportamiento actual.</p>

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	<p>Cambiado el título del control, de Connections a Elasticsearch, los dominios deben cifrarse con la versión TLS 1.2 a Connections, los dominios de Elasticsearch deben cifrarse con la política de seguridad más reciente. TLS Anteriormente, el control solo comprobaba si las conexiones a los dominios de Elasticsearch utilizaban la versión 1.2. TLS El control ahora determina si los dominios de PASSED Elasticsearch están cifrados con la política de seguridad más reciente. TLS El título y la descripción del control se actualizaron para reflejar el comportamiento actual.</p>

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 cambió el título para considerar 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 cambió el título para considerar 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 cambió el título para considerar un nuevo tipo de bucket de S3.
12 de marzo de 2024	[S3.5] Los depósitos de uso general de S3 deberían requerir solicitudes de uso SSL	El cambio de nombre de los buckets S3 debería requerir solicitudes para usar Secure Socket Layer a los buckets de uso general de S3 si requieren solicitudes de uso. SSL Security Hub cambió el título para considerar 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	El cambio de título de los permisos de S3 concedidos a otras Cuentas de AWS políticas de bucket debe restringirse a las políticas de bucket de uso general de S3; las políticas de bucket de uso general deben restringir el acceso a otros. Cuentas de AWS Security Hub cambió el título para considerar 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 cambió el título para considerar 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 cambió el título para considerar un nuevo tipo de bucket de S3.
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 cambió el título para considerar un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
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 cambió el título para considerar un nuevo tipo de bucket de S3.
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 cambió el título para considerar un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
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 cambió el título para considerar un nuevo tipo de bucket de S3.
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 título cambiado de listas de control de acceso de S3 (ACLs) no debe usarse para administrar el acceso de los usuarios a los buckets y no ACLs debe usarse para administrar el acceso de los usuarios a los buckets de uso general de S3. Security Hub cambió el título para considerar un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
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 cambió el título para considerar un nuevo tipo de bucket de S3.
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 cambió el título para considerar un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
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 cambió el título para considerar un nuevo tipo de bucket de S3.
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 cambió el título para considerar un nuevo tipo de bucket de S3.

Fecha del cambio	ID y título de control	Descripción del cambio
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 admite ahora <code>nodejs20.x</code> y <code>ruby3.3</code> como parámetros.
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. Ahora Security Hub admite <code>dotnet8</code> como parámetro.

Fecha del cambio	ID y título de control	Descripción del cambio
5 de febrero de 2024	[EKS.2] EKS los clústeres deberían ejecutarse en una versión compatible de Kubernetes	Security Hub actualizó la versión compatible e más antigua de Kubernetes en la que se puede ejecutar el EKS clúster de Amazon para producir 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	<p>El título modificado o del repositorio fuente de Bitbucket CodeBuild GitHub o el que se URLs debe usar OAuth en el repositorio fuente de CodeBuild Bitbucket no URLs debe contener credenciales confidenciales. Security Hub eliminó la mención de OAuth esto porque otros métodos de conexión también pueden ser seguros. Security Hub eliminó la mención de esto GitHub porque ya no es posible tener un token de acceso personal o un nombre de usuario y contraseña en el repositorio de GitHub origenURLs.</p>

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. 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 RDS instancia de base de datos de Amazon que utiliza uno de los motores de bases de datos compatibles tiene habilitada la protección contra la eliminación. Security Hub admite ahora <code>custom-oracle-ee</code> , <code>oracle-ee-cdb</code> y <code>oracle-se2-cdb</code> como motores 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 admite ahora java21 y python3.12 como parámetros. Security Hub ha dejado de admitir 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 redujo la severidad de este control de CRITICAL a HIGH porque agregar el objeto raíz predeterminado es una recomendación que depende de la aplicación del usuario y de los requisitos específicos.
5 de diciembre de 2023	[EC2.13] Los grupos de seguridad no deberían permitir la entrada desde el 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 deberían permitir la entrada desde el 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	<p>Se ha cambiado el título del control: El registro de bases de datos debe estar habilitado para que las RDS instancias de base de datos publiquen los registros en CloudWatch los registros. Security Hub identificó que este control solo comprueba si los registros se publican en Amazon CloudWatch Logs y no comprueba si RDS los registros están habilitados. El control determina si las RDS instancias de base de datos están configuradas para publicar registros en CloudWatch Logs. PASSED El título del control se ha actualizado para reflejar el comportamiento actual.</p>

Fecha del cambio	ID y título de control	Descripción del cambio
5 de diciembre de 2023	[EKS.8] EKS los clústeres deben tener habilitad o el registro de auditoría	Este control comprueba si los EKS clústeres de Amazon tienen activado el registro de auditoría. La AWS Config regla que utiliza Security Hub para evaluar este control cambió de <code>eks-cluster-logging-enabled</code> a <code>eks-cluster-log-enabled</code> .

Fecha del cambio	ID y título de control	Descripción del cambio
17 de noviembre de 2023	[EC2.19] Los grupos de seguridad no deberían permitir el acceso sin restricciones 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 ha actualizado este control para tener en cuenta las listas de prefijos administrados 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] Las alarmas de CloudWatch deben tener configuradas acciones específicas	Se cambió el título del control: CloudWatch las alarmas deberían tener una acción configurada para el ALARM estado a las CloudWatch alarmas deberían tener configuradas las acciones específicas.
16 de noviembre de 2023	[CloudWatch.16] Los grupos de registros de CloudWatch deben retenerse durante un periodo específico	El título de control modificado de los grupos de CloudWatch registros debe conservarse durante al menos 1 año a los grupos de CloudWatch registros durante un período de tiempo específico.
16 de noviembre de 2023	[Lambda.5] Las funciones VPC Lambda deben funcionar en varias zonas de disponibilidad	Se cambió el título del control: las funciones de VPC Lambda deberían funcionar en más de una zona de disponibilidad a las funciones de VPC Lambda deberían funcionar en varias zonas de disponibilidad.

Fecha del cambio	ID y título de control	Descripción del cambio
16 de noviembre de 2023	[AppSync.2] AWS AppSync debe tener activado 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.
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 EMR clúster de Amazon que 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 debe estar en VPC a OpenSearch. Los dominios no deben ser de acceso público.

Fecha del cambio	ID y título de control	Descripción del cambio
16 de noviembre de 2023	[ES.2] Los dominios de Elasticsearch no deben ser de acceso público	El título de control modificado de los dominios de Elasticsearch debe estar en 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 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 deberían permitir la entrada desde el 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 ha actualizado este control para tener en cuenta las listas de prefijos administrados 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 deberían permitir la entrada desde el 0.0.0.0/0 o :/0 al puerto 3389	EC2.14 comprueba si los grupos de seguridad permiten el acceso de entrada sin restricciones al puerto 3389. Security Hub ha actualizado este control para tener en cuenta las listas de prefijos administrados 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 deberían 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 ha actualizado este control para tener en cuenta las listas de prefijos administrados 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. Ahora Security Hub 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 agregó el parámetro <code>ReplicationType</code> con un valor <code>CROSS-REGION</code> 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] EKS los clústeres deberían ejecutarse en una versión compatible de Kubernetes	Security Hub actualizó la versión compatible e más antigua de Kubernetes en la que se puede ejecutar el EKS clúster de Amazon para producir una conclusión válida. La versión compatible más antigua actual es Kubernetes 1.24.
20 de septiembre de 2023	CloudFront.2 — CloudFront las distribuciones deben tener habilitada la identidad de acceso de origen	Security Hub ha retirado este control y lo ha eliminado de todos los estándares. En su lugar, consulte [CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al 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 no utilizados deberían eliminarse	<p>Security Hub 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</p> <p>Este control produce una comprobación válida si los grupos de seguridad están conectados a EC2 instancia 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.</p>

Fecha del cambio	ID y título de control	Descripción del cambio
20 de septiembre de 2023	EC2.29: las instancias deben lanzarse en un EC2 VPC	Security Hub ha retirado este control y lo ha eliminado de todos los estándares. Amazon EC2 ha migrado las instancias clásicas a unVPC. 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 lado del servidor	Security Hub ha retirado este control y lo ha eliminado 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 cifrado SS3-S3 o SS3 - del lado del servidor. KMS 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	[EC2.2] Los grupos de seguridad predeterminados de VPC no deben permitir el tráfico entrante o saliente	Se ha cambiado el título del control: El grupo de seguridad VPC predeterminado no debe permitir el tráfico entrante y saliente a Los grupos de seguridad VPC predeterminados no deben permitir el tráfico entrante o saliente.
14 de septiembre de 2023	[IAM.9] La MFA debe estar habilitada para el usuario raíz	El título del control cambiado de Virtual MFA debe estar habilitado para el usuario root y MFA debe estar habilitado para el usuario root.

Fecha del cambio	ID y título de control	Descripción del cambio
14 de septiembre de 2023	Las suscripciones de notificación de eventos de RDS [RDS.19] existentes deben configurarse para los eventos de clúster críticos	Se ha cambiado el título del control: Una suscripción a las notificaciones de RDS eventos debe configurarse para los eventos críticos del clúster a las suscripciones de notificaciones de RDS eventos existentes, que deben configurarse para los eventos críticos del clúster.
14 de septiembre de 2023	Las suscripciones de notificación de eventos de RDS [RDS.20] existentes deben configurarse para eventos críticos de instancias de bases de datos	El título del control pasó de Una suscripción a notificaciones de RDS eventos debe configurarse para eventos críticos de instancias de bases de datos a suscripciones de notificaciones de RDS eventos existentes que deben configurarse para eventos críticos de instancias de bases de datos.

Fecha del cambio	ID y título de control	Descripción del cambio
14 de septiembre de 2023	[WAF.2] Las reglas regionales AWS WAF clásicas deben tener al menos una condición	El cambio del título de control de una regla WAF regional debe tener al menos una condición a que las reglas regionales AWS WAF clásicas deben tener al menos una condición.
14 de septiembre de 2023	[WAF.3] Los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla	Cambiado el título de control de un grupo de reglas WAF regionales debe tener al menos una regla a los grupos de reglas regionales AWS WAF clásicos deben tener al menos una regla.
14 de septiembre de 2023	[WAF.4] La web regional AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas	El título del control cambiado de una web WAF regional ACL debe tener al menos una regla o grupo de reglas a una web regional 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	[WAF.6] Las reglas globales AWS WAF clásicas deben tener al menos una condición	Se ha cambiado el título del control de una regla WAF global que debe tener al menos una condición a que las reglas globales AWS WAF clásicas deben tener al menos una condición.
14 de septiembre de 2023	[WAF.7] Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla	Se cambió el título del control de Un grupo de reglas WAF globales debe tener al menos una regla a Los grupos de reglas globales AWS WAF clásicos deben tener al menos una regla.
14 de septiembre de 2023	[WAF.8] La web global AWS WAF clásica ACLs debe tener al menos una regla o grupo de reglas	Se ha cambiado el título del control de Una web WAF global que ACL 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	[WAF.10] la AWS WAF web ACLs debe tener al menos una regla o grupo de reglas	El título del control cambiado de A WAFv2 web ACL 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	[WAF.11] El ACL registro AWS WAF web debe estar habilitado	El título de control modificado, de AWS WAF la versión 2 del ACL registro web debe estar activado a la versión 2, el ACLregistro AWS WAF web debe estar activado.

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 el cifrado del lado 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 actualizó este control para incluir el cifrado de doble capa del lado del servidor con KMS claves (DSSE-KMS). El control produce un resultado válido cuando un bucket de S3 se cifra con SSE-S3KMS, SSE-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 actualizó este control para incluir el cifrado de doble capa del lado del servidor con KMS claves (DSSE-KMS). El control produce un resultado válido cuando un bucket de S3 se cifra con SSE - KMS o DSSE -KMS.
9 de junio de 2023	[EKS.2] EKS los clústeres deberían ejecutarse en una versión compatible de Kubernetes	EKS.2 comprueba si un EKS clúster de Amazon 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. Ahora Security Hub admite <code>ruby3.2</code> como parámetro.
5 de junio de 2023	[APIGateway.5] Los datos de la REST API caché de API Gateway deben cifrarse en reposo	APIGateway.5. Comprueba si todos los métodos de las REST API etapas de Amazon API Gateway están cifrados en reposo. Security Hub 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. Ahora Security Hub admite <code>java17</code> 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 ha dejado de admitir <code>nodejs12.x</code> como parámetro.

Fecha del cambio	ID y título de control	Descripción del cambio
23 de abril de 2023	[ECS.10] Los servicios de ECS Fargate deberían ejecutarse en la última versión de la plataforma Fargate	ECS.10 comprueba si los servicios de Amazon ECS Fargate utilizan la versión más reciente de la plataforma Fargate. Los clientes pueden implementar Amazon ECS ECS directamente o mediante CodeDeploy. Security Hub actualizó este control para generar resultados aprobados cuando se utilizan CodeDeploy para implementar los servicios de ECS Fargate.

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 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. Ahora Security Hub 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 ha dejado de admitir dotnetcore3.1 como parámetro.

Fecha del cambio	ID y título de control	Descripción del cambio
17 de abril de 2023	<u>Las instancias RDS [RDS.11] deben tener habilitadas las copias de seguridad automáticas</u>	<p>RDS.11 comprueba si RDS las instancias de Amazon tienen habilitadas las copias de seguridad automáticas, con un período de retención de las copias de seguridad superior o igual a siete días. Security Hub 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 período de retención de las copias de seguridad al crear réplicas de lectura. Las réplicas de lectura se crean con un período de retención predeterminado de la copia de seguridad de 0.</p>

Historial de documentos de la Guía del usuario de AWS Security Hub

En la siguiente tabla se describen las actualizaciones de la documentación de AWS Security Hub.

Note

En el caso de las versiones de control de seguridad, la fecha especificada es la fecha en que los controles estarán disponibles en todas las cuentas y regiones. Los controles pueden tardar entre 1 y 2 semanas en llegar a todas las cuentas y regiones.

Cambio	Descripción	Fecha
Nuevos controles de seguridad	<p>Security Hub lanzó 37 controles nuevos para el estándar AWS de etiquetado o de recursos. Security Hub también lanzó los siguientes controles nuevos:</p> <ul style="list-style-type: none"> • 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” 	22 de enero de 2025
Nuevo control de seguridad	Security Hub publicó la versión EC2.172 La configuración de	15 de enero de 2025

[acceso público del bloque de EC2 VPC debería bloquear el tráfico de las puertas de enlace de Internet.](#)

[Nuevos controles de seguridad](#)

Están disponibles los siguientes controles 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 es compatible con PCI DSS v4.0.1](#)

Security Hub 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](#).

11 de diciembre de 2024

[Security Hub recibe los resultados de la secuencia de GuardDuty ataque](#)

Security Hub 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 es compatible con la nueva Región de AWS](#)

Security Hub ya está disponible en la región de Asia Pacífico (Malasia). Algunos controles de seguridad tienen limitaciones regionales. Para ver una lista de los controles que no están disponibles en esta región, consulte [Límites regionales de los controles de Security Hub](#).

22 de noviembre de 2024

[Cambios en la configuración.1](#)

Security Hub 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 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 de Security Hub](#).

20 de noviembre de 2024

[Nuevos controles de seguridad](#)

Están disponibles los siguientes controles nuevos de Security Hub. Estos controles forman parte de AWS Foundational Security Best Practices v1.0.0 y 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. 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 nuevos de Security Hub.

18 de octubre de 2024

- [the section called “\[AppSync .1\] las AWS AppSync API cachés deben cifrarse en reposo”](#)
- [the section called “\[AppSync .6\] AWS AppSync API Las cachés deben cifrarse en tránsito”](#)
- [the section called “\[EC2.170 \] Las plantillas de EC2 lanzamiento deben utilizar la versión 2 \(\) del Servicio de Metadatos de Instancia IMDSv2”](#)
- [the section called “\[EC2.171 \] Las conexiones EC2 VPN deben tener el registro activado”](#)
- [the section called “\[EFS.8\] los sistemas de EFS archivos 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 SNS temas no deberían permitir el acceso público”](#)

Nuevos controles de seguridad

Están disponibles los siguientes controles nuevos de Security Hub. 3 de octubre de 2024

- the section called “[ECS.16] Los conjuntos de ECS tareas no deben asignar automáticamente direcciones IP públicas”
- the section called “[GuardDuty.7] La monitorización del GuardDuty EKS tiempo de ejecución 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 MSK Connect deben estar cifrados 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 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 “\[DataSync.1\] Las tareas de DataSync deben tener el registro habilitado”](#)
- [the section called “\[EFS.7\] los sistemas de EFS archivos 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 usuarios de Workspace deben estar cifrados en reposo”](#)
- [the section called “\[WorkSpaces.2\] Los volúmenes raíz](#)

[de WorkSpaces deben estar cifrados en reposo”](#)

[Nuevo panel de resultados](#)

El [nuevo panel de resultados](#) en la consola de Security Hub ayuda a tomar medidas rápidamente en relación con los resultados, revisar los detalles de los recursos y el historial de resultados, y encontrar otra información pertinente sobre un resultado.

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 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 estar cifrados en reposo”](#)
- [the section called “\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización IAM”](#)
- [the section called “\[DMS.11\] DMS Los puntos finales de MongoDB deberían tener habilitado un mecanismo de autenticación”](#)
- [the section called “\[DMS.12\] DMS Los puntos finales de Redis deberían estar habilitados OSS TLS”](#)
- [the section called “\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito”](#)
- [the section called “\[EFS.6\] Los destinos de EFS montaje no deben estar](#)

- asociados a una subred pública”
- the section called “[EKS.3] los EKS clústeres 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 terminales de SageMaker IA 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 organización de AWS”
- the section called “[Transfer.2] Los servidores Transfer Family no deben usar el FTP protocolo para la conexión de puntos finales”

Nuevos controles de seguridad

Ya están disponibles los siguientes controles nuevos de Security Hub:

11 de julio de 2024

- [the section called “\[GuardDuty.5\] La supervisión del registro de GuardDuty EKS auditoría debe estar habilitada”](#)
- [the section called “\[GuardDuty.6\] La protección 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 GuardDuty RDS protección debe estar habilitada”](#)
- [the section called “\[GuardDuty.10\] La protección 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 ECR escaneo de Amazon Inspector debe estar activado”](#)
- [the section called “\[Inspector.3\] El análisis de código](#)

de Lambda en Amazon Inspector debe estar habilitado”

- the section called “[Inspector.4] El análisis estándar de Lambda en Amazon Inspector debe estar habilitado”

[Publicación de CIS AWS Foundations Benchmark v3.0.0](#)

13 de mayo de 2024

Security Hub lanzó el [Indicador de referencia de AWS v3.0.0 de Center for Internet Security \(CIS\)](#). La versión incluye los siguientes controles nuevos, así como asignaciones a varios controles existentes.

- [the section called “\[EC2.53\] los grupos de EC2 seguridad no deberían permitir la entrada desde el 0.0.0.0/0 a los puertos de administración remota del servidor”](#)
- [the section called “\[EC2.54\] Los grupos EC2 de seguridad no deberían permitir la entrada desde: :/0 a los puertos de administración remota del servidor”](#)
- [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 la política adjunta 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

Ya están disponibles los siguientes controles nuevos de Security Hub:

3 de mayo de 2024

- [the section called “\[DataFirehose.1\] Los flujos de entrega de Firehose deben estar cifrados en reposo”](#)
- [the section called “\[DMS.10\] DMS Los puntos finales de las bases de datos de Neptune deben tener habilitada la autorización IAM”](#)
- [the section called “\[DMS.11\] DMS Los puntos finales de MongoDB deberían tener habilitado un mecanismo de autenticación”](#)
- [the section called “\[DMS.12\] DMS Los puntos finales de Redis deberían estar habilitados OSS TLS”](#)
- [the section called “\[DynamoDB.7\] Los clústeres del Acelerador de DynamoDB deben estar cifrados en tránsito”](#)
- [the section called “\[EFS.6\] Los destinos de EFS montaje no deben estar asociados a una subred pública”](#)
- [the section called “\[EKS.3\] los EKS clústeres 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 terminales de SageMaker IA deben tener un recuento

	<p>inicial de instancias superior a 1”</p> <ul style="list-style-type: none">• the section called “[Service Catalog.1] Las carteras de Service Catalog solo deben compartirse dentro de una organización de AWS”• the section called “[Transfer.2] Los servidores Transfer Family no deben usar el FTP protocolo para la conexión de puntos finales”	
AWS Estándar de etiquetado de recursos	La Pauta de etiquetado de los recursos de AWS de Security Hub ya está disponible de forma general, junto con los nuevos controles que se aplican a la pauta.	30 de abril de 2024
Actualización de la política administrada existente	Security Hub actualizó la política AWS gestionada denominada AmazonSecurityHubFullAccess para obtener información detallada sobre los precios Servicios de AWS y los productos.	24 de abril de 2024
Configuración en contexto de los parámetros de control	Si utiliza la configuración centralizada, ahora puede configurar los parámetros de control en contexto desde la página de detalles de un control de la consola de Security Hub.	29 de marzo de 2024

Actualización de la política administrada existente	Security Hub actualizó la política administrada de AWS denominada AWSSecurityHubReadOnlyAccess mediante el agregado de un campo Sid.	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
Disponibilidad de Security Hub en la región Oeste de Canadá (Calgary)	Security Hub ya está disponible en la región Oeste de Canadá (Calgary). Ya están disponibles en esta región todas las características de Security Hub, 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

Ya están disponibles los siguientes controles nuevos de Security Hub:

14 de diciembre de 2023

- the section called “Los puntos de recuperación de [Backup.1] AWS Backup deben estar cifrados en reposo”
- the section called “[DynamoDB.6] Las tablas de DynamoDB deben tener la protección contra eliminación habilitada”
- the section called “[EC2.51] Los puntos finales de EC2 Client VPN deben tener habilitado el registro de conexiones de clientes”
- the section called “[EKS.8] EKS los clústeres 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] FSx para sistemas de ZFS archivos abiertos, debe configurarse para copiar etiquetas a copias de seguridad y volúmenes”

- [the section called “\[Macie.1\] Amazon Macie debe estar habilitado”](#)
- [the section called “\[MSK.2\] MSK los clústeres deben 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 “\[Network Firewall.1\] Los 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 cubos de uso general de S3 deberían tener habilitada la función de eliminación MFA”](#)

[Enriquecimiento de resultados](#)

Security Hub agregó los nuevos campos `AwsAccountName` de búsqueda y `ApplicationName` al formato de búsqueda AWS de seguridad (ASFF). `ApplicationArn`

27 de noviembre de 2023

[Mejoras en el panel Resumen](#)

Ahora puede acceder a más widgets del panel en la página Resumen de la consola de Security Hub, guardar los conjuntos de filtros del 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 la configuración central, el administrador delegado del Security Hub puede configurar el Security Hub, los estándares y los controles en varias cuentas, unidades organizativas (OUs) y regiones de la organización.

27 de noviembre de 2023

[Actualizaciones a políticas administradas](#)

Security Hub agregó nuevos permisos a la política administrada `AWSecurityHubServiceRolePolicy`, los cuales le permiten leer y actualizar las 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 controles específicos 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 actualizó `AWSecurityHubFullAccess` y `AWSecurityHubOrganizationsAccess` gestionó las políticas que le permiten utilizar, respectivamente, las funciones de Security Hub 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 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 agregó un nuevo permiso de etiquetado a la política `AWSecurityHubServiceRolePolicy` administrada que permite a Security Hub leer las etiquetas de recursos relacionadas con los resultados.

7 de noviembre de 2023

Nuevos controles de seguridad

Ya están disponibles los siguientes controles nuevos de Security Hub:

10 de octubre de 2023

- [the section called “\[AppSync.5\] AWS AppSync APIs GraphQL no debe autenticarse con claves API”](#)
- [the section called “\[DMS.6\] las instancias de DMS replicación deben tener habilitada la actualización automática de las versiones secundarias”](#)
- [the section called “\[DMS.7\] las tareas de DMS replicación de la base de datos de destino deben tener habilitado el registro”](#)
- [the section called “\[DMS.8\] las tareas de DMS replicación de la base de datos de origen deben tener el registro activado”](#)
- [the section called “\[DMS.9\] Los DMS puntos finales deben utilizar 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 ECS tareas 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] MSK Los clústeres deben cifrarse en tránsito entre los nodos intermediarios”
- 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 firewalls de Network Firewall \[NetworkFirewall.9\] 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 “\[Route53 .2\] Las zonas alojadas públicamente de Route 53 deberían registrar las consultas DNS”](#)
- [the section called “\[WAF.12\] AWS WAF las reglas deben tener las CloudWatch métricas habilitadas”](#)

[Actualizaciones a la política administrada](#)

Security Hub agregó nuevas acciones de Organizat ions (Organizaciones) a la AWSSecurityHubServiceRolePolicy política administrada que permiten a Security Hub recuperar información de cuentas y unidades organizativas (OU). También agregamos nuevas acciones de Security Hub que permiten a Security Hub 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 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 bases de datos de Neptune deben tener habilitada la autenticación de bases de datos 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 controles consolidados y los hallazgos 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 Controls de la consola 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 Controls de la consola 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.

28 de agosto de 2023

[Security Hub está disponible en la región de Israel \(Tel Aviv\)](#)

Security Hub ya está disponible en Israel (Tel Aviv). Ya están disponibles en esta región todas las características de Security Hub, con la excepción de algunos controles de seguridad. Para obtener más información, consulte [Disponibilidad de controles por región](#).

8 de agosto de 2023

Nuevos controles de seguridad

Ya están disponibles los siguientes controles 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 bases de datos de Neptune deben tener habilitada la autenticación de bases de datos 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 ahora ofrece reglas de automatización que actualizan automáticamente los resultados según los criterios que especifique.

13 de junio de 2023

[Nueva integración de terceros](#)

Snyk es una nueva integración de terceros que envía los resultados a Security Hub.

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 de Security Hub existentes a Service-Managed Standard: AWS Control Tower

12 de junio de 2023

- [the section called “\[Account .1\] La información de contacto de seguridad debe proporcionarse para una 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 de API Gateway V2”](#)
- [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 “\[ELB.1\] Application Load Balancer debe configurarse para redirigir todas las HTTP solicitudes a HTTPS”](#)
- [the section called “Los clústeres de Redshift](#)

- [Redshift.10] deben cifrarse en reposo”
- the section called “[SageMaker.2] Las instancias de SageMaker AI notebook deben lanzarse en una VPC personalizada”
 - the section called “[SageMaker.3] Los usuarios no deberían tener acceso root a las instancias de SageMaker AI Notebook”
 - the section called “[WAF.10] la AWS WAF web ACLs debe tener al menos una regla o grupo de reglas”

Nuevos controles de seguridad

Ya están disponibles los siguientes controles nuevos de Security Hub:

6 de junio de 2023

- the section called “[ACM.2] RSA los certificados gestionados por ACM deben utilizar una longitud de clave de al menos 2048 bits”
- the section called “[AppSync .2] AWS AppSync debe tener activado el registro a nivel de campo”
- the section called “[CloudFront.13] CloudFront las distribuciones deben usar el control de acceso al 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 disponible en Asia-Pacífico \(Melbourne\)](#)

Security Hub ya está disponible en la región de Asia-Pacífico (Melbourne). Ya están disponibles en esta región todas las características de Security Hub, 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 ahora puede rastrear el historial de un resultado durante los últimos 90 días.

4 de mayo de 2023

[Nuevos controles de seguridad](#)

Ya están disponibles los siguientes controles nuevos de Security Hub:

29 de marzo de 2023

- [the section called “\[EKS.1\] Los puntos finales de los EKS clústeres no deben ser de acceso público”](#)
- [the section called “\[ELB.16\] Los balanceadores de carga de aplicaciones deben estar asociados a una web AWS WAF ACL”](#)
- [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 habilidad o 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 disponible en una nueva versión Regiones de AWS](#)

Security Hub ya está disponible en las regiones de 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 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 agregó los siguientes controles de seguridad, que son aplicables al estándar NIST 800-53:

- [the section called “\[Account .2\] Cuentas de AWS debe ser parte de una organización de AWS Organizations”](#)
- [the section called “\[CloudWatch.15\] Las alarmas de CloudWatch deben tener configuradas acciones específicas”](#)
- [the section called “\[CloudWatch.16\] Los grupos de registros de CloudWatch deben retenerse durante un periodo específico”](#)
- [the section called “\[CloudWatch.17\] Las acciones de alarma de CloudWatch 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 respaldo”](#)
- 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 habilitado o el control de versiones”](#)
- [the section called “\[WAF.11\] El ACL registro AWS WAF web debe estar habilitado”](#)

[National Institute of Standards and Technology \(NIST, Instituto Nacional de Estándares y Tecnología\) 800-53, Rev. 5](#)

Security Hub 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 Controles de la consola de Security Hub muestra todos los controles de todos 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 nuevos de Security Hub. Algunos controles tienen restricciones regionales. 16 de febrero de 2023

- the section called “[ElastiCache.1] Los clústeres ElastiCache (RedisOSS) 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

[\(RedisOSS\) de versiones anteriores deberían tener Redis activado OSS AUTH”](#)

- [the section called “\[Elasticache.7\] los ElastiCache clústeres no deben usar el grupo de subredes predeterminado”](#)

[Nuevos campos del ASFF](#)

Se ha añadido Security Hub ProductFields. ArchivalReasonsSe ProductFields ha agregado Security Hub. ----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 ha añadido el cumplimiento. Associate dStandards 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 de Security Hub para ver los resultados que Amazon Inspector envía a Security Hub.

14 de enero de 2023

Security Hub está disponible en Oriente Medio (UAE)	Security Hub ya está disponible en Oriente Medio (UAE). Algunos controles tienen límites regionales.	12 de enero de 2023
Se agregó la integración de terceros con MetricStream	Security Hub ahora admite la integración de terceros con MetricStream en todas las regiones excepto China y AWS GovCloud (US).	11 de enero de 2023
Se ha incrementado el límite de cuentas organizativas	Security Hub ahora es compatible con hasta 11,000 cuentas de miembros por cada cuenta de administrador de Security Hub por región.	27 de diciembre de 2022
ElasticBeanstalk3. Retirado	Security Hub anuló el control [ElasticBeanstalk.3] Elastic Beanstalk debería transmitir los CloudWatch registros desde el estándar FSBP en todas las regiones.	21 de diciembre de 2022
Security Hub agrega nuevos controles de seguridad	Los nuevos controles 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 planea lanzar dos nuevas características: vista de controles consolidada y resultados 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 Security Hub al recibir los resultados del Security Hub.

29 de noviembre de 2022

[Support for Service-Managed Standard: AWS Control Tower](#)

Security Hub es compatible con 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 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 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 a Security Hub en todas las regiones disponibles.	17 de noviembre de 2022
Support para CIS AWS Foundations Benchmark v1.4.0	Security Hub 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
Anuncios de Support for Security Hub en AWS GovCloud (US)	Ahora puede suscribirse a los anuncios de Security Hub 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.	3 de octubre de 2022
AWS Security Hub añade un nuevo control de seguridad	El nuevo Security Hub 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
Suscríbese a los anuncios de Security Hub	Ahora puede suscribirse a los anuncios de Security Hub con Amazon Simple Notification Service (Amazon SNS) para recibir notificaciones sobre Security Hub.	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 del Security Hub y JFrog es una integración de terceros que envía las conclusiones a Security Hub.	26 de julio de 2022
<u>EC2.27 está retirado</u>	Security Hub 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
<u>Lambda.2 ya no es compatible con python3.6</u>	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

<u>AWS Security Hub agrega nuevos controles de seguridad</u>	Los nuevos controles de Security Hub están disponibles para los clientes que hayan activado el estándar FSBP. Algunos controles tienen <u>restricciones regionales</u> .	22 de junio de 2022
<u>AWS Security Hub apoya a una nueva región</u>	Security Hub ya está disponible en Asia-Pacífico (Yakarta). Algunos controles no están disponibles en esta región.	7 de junio de 2022
<u>Integración mejorada entre AWS Security Hub y AWS Config</u>	Los usuarios de Security Hub pueden ver los resultados de las evaluaciones de AWS Config reglas como hallazgos en Security Hub.	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 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

CompanyName y ahora ProductName son atributos de primer nivel	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
Se agregaron nuevos controles al estándar de mejores prácticas de seguridad AWS fundamentales	Se agregaron 5 controles nuevos al estándar de AWS de prácticas recomendadas de seguridad fundamentales.	31 de marzo de 2022
Se agregaron nuevos objetos de detalles de recursos al ASFF	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 AWS de prácticas recomendadas de seguridad fundamentales.	16 de marzo de 2022

<u>Se agregaron nuevos controles al estándar AWS fundamental de mejores prácticas de seguridad y al estándar de seguridad de datos del sector de las tarjetas de pago (PCI DSS)</u>	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
<u>Se agregó un nuevo campo al ASFF</u>	Se agregó un nuevo campo: Muestra.	26 de enero de 2022
<u>Se agregó la integración con AWS Health</u>	AWS Health utiliza la mensajería de service-to-service eventos para enviar las conclusiones a Security Hub.	19 de enero de 2022
<u>Se agregó la integración con AWS Trusted Advisor</u>	Trusted Advisor envía los resultados de sus comprobaciones al Security Hub a medida que éste los encuentra . Security Hub 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: AwsNetworkFirewallFirewall , AwsNetworkFirewallPolicy , y AwsNetworkFirewallRuleGroup .

20 de diciembre de 2021

Se agregó soporte para la nueva versión de Amazon Inspector	Security Hub está integrado con la nueva versión de Amazon Inspector y con Amazon Inspector Classic. Amazon Inspector envía los resultados a Security Hub.	29 de noviembre de 2021
Se modificó la gravedad de EC2 .19	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 ahora ofrece una integración con Sonrai Dig. Sonrai Dig monitorea los entornos de nube para identificar los riesgos de seguridad. Sonrai Dig envía los resultados a Security Hub.	12 de noviembre de 2021
Comprobación actualizada de los controles CIS 2.1 y CloudTrail .1	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	Security Hub ahora está integrado con los puntos finales de VPC AWS PrivateLink y es compatible con ellos.	3 de noviembre de 2021

[Se agregaron controles al estándar de AWS mejores prácticas de 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 los resultados de Security Hub.

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 `AwsElasticLoadBalancingV2LoadBalancer`. 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: <code>AwsEc2VpcEndpointService</code> , <code>AwsEcrRepository</code> , <code>AwsEksCluster</code> , <code>AwsOpenSearchServiceDomain</code> , <code>AwsWafRateBasedRule</code> , <code>AwsWafRegionalRateBasedRule</code> , <code>AwsXrayEncryptionConfig</code>	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 <code>dotnetcore2.1</code> tiempo de ejecución de [Lambda.2] Las funciones Lambda deberían usar tiempos de ejecución compatibles.	6 de octubre de 2021
Nuevo nombre para la integración de Check Point	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
Se eliminó la integración con Alcide	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 con Organizations (Organizaciones) ya está disponible en China (Pekín) 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
<u>Se eliminaron los tiempos de ejecución obsoletos del control Lambda.2</u>	En el estándar AWS Foundational Security Best Practices , se eliminaron los tiempos de ejecución 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 validación del archivo de CloudTrail 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 Foundational Security Best Practices, ECS.1 ahora tiene un parámetro establecido en `SkipInactiveTaskDefinitions true`. Esto garantiza que el control solo compruebe las definiciones de tareas activas. Para Lambda.2, se agregó Python 3.9 a la lista de tiempos de ejecución. Ahora, SSM.1 comprueba tanto las instancias 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 ahora ofrece una integración con HackerOne Vulnerability Intelligence. La integración envía los resultados a Security Hub.

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 <code>Vulnerabilities</code> 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 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 retira el control [Lambda.4] Las funciones de Lambda deberían tener configurada una cola de mensajes fallidos. Cuando se retira un control, deja de mostrarse en la consola y Security Hub no realiza revisiones.	31 de agosto de 2021
Retirar la PCI. EC23. Control	Security Hub 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 no realiza revisiones.	27 de agosto de 2021
Cambio en la forma en que Security Hub envía los resultados a las acciones personalizadas	Quando envías los resultados a una acción personalizada, Security Hub ahora envía cada hallazgo de forma separada. Security Hub Findings - Custom ActionEvento .	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 no pudo realizar una revisión con un tiempo 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 con Firewall Manager ya 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 ahora ofrece integraciones con Caveonix Cloud y Forcepoint Cloud Security Gateway. Ambas integraciones envían los resultados a Security Hub.

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 AWS prácticas de 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 `AWSecurityHubServiceRolePolicy` , gestionada para que se aplique a todos los recursos.

14 de julio de 2021

<u>Se agregaron controles al estándar básico de mejores prácticas de seguridad AWS</u>	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
<u>Se agregaron nuevos códigos de motivo de estado de cumplimiento para los resultados de control</u>	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
<u>Se agregó la integración con AWS Chatbot</u>	Se agregó la integración con AWS Chatbot. Security Hub envía los resultados a AWS Chatbot.	30 de junio de 2021
<u>Se agregó un nuevo permiso a la política de administración de funciones vinculadas al servicio</u>	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 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](#)

Se agregó información sobre cómo gestiona Security Hub las cuentas suspendidas en 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 Lambda.2 control.

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. NETSCOUT Cyber Investigator envía los resultados a Security Hub.

7 de junio de 2021

[Se agregaron detalles para AWSSecurityHubServiceRolePolicy](#)

Se actualizó la sección de políticas administradas para agregar detalles de la política administrada existente AWSSecurityHubServiceRolePolicy , que utiliza la función vinculada al servicio Security Hub.

4 de junio de 2021

[Nueva integración con Jira Service Management](#)

El conector de administración de AWS 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 los resultados correspondientes en Security Hub.

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 a Security Hub.

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 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 AWS Systems Manager Explorer y OpsCenter	Security Hub ahora admite una integración con Systems Manager Explorer y OpsCenter. La integración recibe los resultados de Security Hub y actualiza esos resultados en Security Hub.	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 resultados que recibe de Security Hub.	22 de abril de 2021
Se cambió “cuenta maestra” a “cuenta de administrador”	El término “cuenta maestra” se cambia a “cuenta de administrador”. El término también se cambia en la consola de Security Hub y la API.	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 con ahora GuardDuty es compatible en las regiones de China (Beijing) y China (Ningxia).	5 de abril de 2021
Se agregó nodejs14.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 nodejs14.x .	30 de marzo de 2021
Security Hub se lanzó en Asia-Pacífico (Osaka)	Security Hub 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 resultados confidenciales a Security Hub.	23 de marzo de 2021

[¿Se está realizando la transición a la gestión de AWS Organizations cuentas?](#)

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

<u>Nuevo objeto en el ASFF que permite buscar proveedor es para actualizar campos específicos</u>	El nuevo objeto <code>FindingProviderFields</code> del ASFF se utiliza en <code>BatchImportFindings</code> para proporcionar valores para <code>Confidence</code> , <code>Criticality</code> , <code>RelatedFindings</code> , <code>Severity</code> , y <code>Types</code> . Los campos originales solo deben actualizarse utilizando <code>BatchUpdateFindings</code> .	18 de marzo de 2021
<u>Nuevo <code>DataClassification</code> objeto para los recursos en el ASFF</u>	El nuevo <code>Resources.DataClassification</code> objeto del ASFF se utiliza para proporcionar información sobre los datos confidenciales que se detectaron en el recurso.	18 de marzo de 2021
<u>Valor <code>CONFIG_REURNS_NOT_APPLICABLE</code> agregado a los códigos de estado de cumplimiento disponibles</u>	Para el estado de cumplimiento <code>NOT_AVAILABLE</code> , se eliminó el código de motivo <code>RESOURCE_NO_LONGER_EXISTS</code> y se agregó el código de motivo <code>CONFIG_REURNS_NOT_APPLICABLE</code> .	16 de marzo de 2021

[Nueva política gestionada para la integración con AWS Organizations](#)

Una nueva política gestionada, `AWSecurityHubOrganizationsAccess`, proporciona a las Organizaciones (Organizaciones) los permisos que necesitan la cuenta de administración de la organización y la cuenta de administrador delegada de Security Hub.

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 SecureCloud DB](#)

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 a Security Hub.

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

Se eliminó el control RDS.11	Se eliminó el control RDS.11 del estándar de prácticas recomendadas de seguridad fundamentales.	3 de marzo de 2021
Integración actualizada para Turbot	La integración de Turbot se actualizó para enviar y recibir resultados.	26 de febrero de 2021
Se agregaron controles al estándar de prácticas recomendadas de seguridad fundamentales	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
Se agregó un filtro ProductArn opcional a la DescribeProducts API	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
Nueva integración con Antivirus para Amazon S3 de Cloud Storage Security	La integración con Antivirus para Amazon S3 envía los resultados del análisis de virus a Security Hub como resultados.	27 de enero de 2021

[Se actualizó el proceso de cálculo de la puntuación de seguridad de las cuentas de administrador](#)

En el caso de una cuenta de administrador, Security Hub 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 restablece automáticamente el estado del flujo de trabajo desde NOTIFIED o RESOLVED hasta NEW si un resultado archivado se activa, o si el estado de cumplimiento de una búsqueda cambia de PASSED a, ya sea, FAILED, WARNING, o 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](#)

Para los resultados que se generan a partir de los controles, se agregó información sobre el contenido del objeto ProductFields en Formato de resultados de seguridad de AWS (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 de 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 reciben un hallazgo del Security Hub. Las actualizaciones de estos incidentes o problemas dan lugar a actualizaciones de los resultados en Security Hub.	11 de diciembre de 2020
Nueva integración con AWS Audit Manager	Security Hub ahora ofrece una integración con AWS Audit Manager. La integración permite a Audit Manager recibir los resultados basados en el control de parte de Security Hub.	8 de diciembre de 2020
Nueva integración con Aqua Security Kube-bench	Security Hub agregó una integración con Aqua Security Kube-bench. La integración envía los resultados a Security Hub.	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 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 de Security Hub, quien determina qué cuentas de organización habilitar en Security Hub. 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 ahora admite integraciones con cloudfire.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 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

Se lanzó Security Hub en China (Pekín) y China (Ningxia)	Security Hub 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 CloudWatch Events por 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 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. VM-Series recibe resultados de Security Hub.	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 , AwsElbLoadBalancer , 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 El administrador de parches ahora está integrado con Security Hub. Patch Manager envía los resultados a Security Hub cuando las instancias de la flota de un cliente no cumplen con su estándar de conformidad para parches.

22 de septiembre de 2020

[Se agregaron nuevos controles al estándar de mejores prácticas de seguridad AWS 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 ya no genera resultados a nivel de cuenta para un control. Solo se generan resultados a nivel de recursos.

1 de septiembre de 2020

[¿Nuevo PatchSummary objeto en 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 ahora está integrado con RSA Archer. RSA Archer recibe los resultados de Security Hub.

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

<u>Se agregaron campos a AwsRdsDbInstance</u>	Se agregaron varios atributos al AwsRdsDbInstance objeto que se encuentra abajo de Resources.Details .	18 de agosto de 2020
<u>Se ha actualizado la forma en la que Security Hub determina el estado general de un control</u>	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
<u>Se actualizó la forma en que Security Hub calcula la puntuación de seguridad de un estándar</u>	Al calcular la puntuación de seguridad de un estándar, Security Hub 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, 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 resultados de los controles, si <code>Compliance.Status</code> es <code>PASSED</code> , entonces Security Hub establece automáticamente <code>Workflow.Status</code> 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 Security Hub. Incluye habilitar Security Hub, administrar hallazgos , administrar estándares y controles, administrar integraciones de productos y deshabilitar Security Hub.	24 de junio de 2020

Nuevo Severity. Original atributo en el ASFF	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
Nuevo Compliance. StatusReasons objeto en el ASFF para obtener detalles sobre el estado de un control	Se agregó el objeto <code>Compliance.StatusReasons</code> , que proporciona contexto adicional para el estado actual de un control.	20 de mayo de 2020
Nuevo AWS estándar fundamental de mejores prácticas de seguridad	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
Nueva opción de consola para actualizar el estado de flujo de trabajo para un resultado	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 muestra ahora la categoría de integración y si cada integración envía o recibe resultados de Security Hub. 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 de Security Hub para el Payment Card Industry Data Security Standard (PCI DSS). Cuando este estándar está habilitado, Security Hub realiza comprobaciones automatizadas de los controles relacionados con los requisitos de PCI DSS.	13 de febrero de 2020
AWS Actualizaciones del formato de búsqueda de 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 Security Hub](#)

Se actualizaron algunas descripciones y se agregaron nuevos términos a [Conceptos de Security Hub](#).

21 de septiembre de 2019

[AWS Versión de disponibilidad general de Security Hub](#)

Actualizaciones de contenido para reflejar las mejoras realizadas a Security Hub durante el período de versión preliminar.

25 de junio de 2019

[Se agregaron pasos de corrección para las verificaciones de CIS AWS Foundations](#)

Se agregaron pasos de corrección a los [estándares de seguridad compatibles con AWS Security Hub](#).

15 de abril de 2019

[Versión preliminar de AWS Security Hub](#)

Publicación de la versión preliminar de la AWS Guía del usuario de Security Hub.

18 de noviembre de 2018

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la versión original de inglés, prevalecerá la versión en inglés.