Guía de implementación

Respuesta de seguridad automatizada en AWS

Respuesta de seguridad automatizada en AWS: Guía de implementación

Table of Contents

Aborde automáticamente las amenazas de seguridad con acciones de respuesta y corrección predefinidas en AWS Security Hub

Esta guía de implementación proporciona información general sobre la solución Automated Security Response on AWS, su arquitectura y componentes de referencia, las consideraciones para planificar la implementación y los pasos de configuración para implementar la solución Automated Security Response on AWS en la nube de Amazon Web Services (AWS).

Utilice esta tabla de navegación para encontrar rápidamente las respuestas a estas preguntas:

Si quiere…	Lea…
Conozca el costo de ejecutar esta solución	Costo
Comprenda las consideraciones de seguridad de esta solución	Seguridad
Sepa cómo planificar las cuotas de esta solución	Cuotas
Conozca qué regiones de AWS son compatibl es con esta solución	Regiones de AWS admitidas
Consulte o descargue la CloudFormation plantilla de AWS incluida en esta solución para implementar automáticamente los recursos de infraestructura (la «pila») de esta solución	CloudFormation Plantillas de AWS
Acceda al código fuente y, si lo desea, utilice el AWS Cloud Development Kit (AWS CDK) para implementar la solución.	GitHub repositorio

La continua evolución de la seguridad requiere medidas proactivas para proteger los datos, lo que puede hacer que la reacción de los equipos de seguridad sea difícil, costosa y lenta. La solución Automated Security Response en AWS le ayuda a reaccionar rápidamente para abordar los

problemas de seguridad al proporcionar respuestas predefinidas y acciones correctivas basadas en las mejores prácticas y los estándares de conformidad del sector.

Automated Security Response en AWS es una solución de AWS que funciona con AWS Security Hub para mejorar su seguridad y ayudar a alinear sus cargas de trabajo con las prácticas recomendadas del pilar de la seguridad de Well-Architected (0). SEC1 Esta solución facilita a los clientes de AWS Security Hub la resolución de problemas de seguridad habituales y mejora su postura de seguridad en AWS.

Puede seleccionar guías específicas para implementarlas en su cuenta principal de Security Hub. Cada manual contiene las acciones personalizadas necesarias, las funciones de Identity and Access Management (IAM), EventBridge las reglas de Amazon, los documentos de automatización de AWS Systems Manager, las funciones de AWS Lambda y las AWS Step Functions necesarias para iniciar un flujo de trabajo de remediación en una sola cuenta de AWS o en varias cuentas. Las correcciones funcionan desde el menú Acciones de AWS Security Hub y permiten a los usuarios autorizados corregir un hallazgo en todas sus cuentas administradas por AWS Security Hub con una sola acción. Por ejemplo, puede aplicar las recomendaciones del Centro para la Seguridad de Internet (CIS) AWS Foundations Benchmark, un estándar de conformidad para proteger los recursos de AWS, a fin de garantizar que las contraseñas caduquen en un plazo de 90 días y aplicar el cifrado de los registros de eventos almacenados en AWS.

> **Note**
>
> La remediación está destinada a situaciones emergentes que requieren una acción inmediata. Esta solución solo realiza cambios para corregir los hallazgos cuando usted los inicia a través de la consola de administración de AWS Security Hub o cuando se ha habilitado la corrección automática mediante la EventBridge regla de Amazon para un control específico. Para revertir estos cambios, debe volver a colocar los recursos en su estado original de forma manual.
>
> Al corregir los recursos de AWS implementados como parte de la CloudFormation pila, tenga en cuenta que esto podría provocar una desviación. Siempre que sea posible, corrija los recursos de la pila modificando el código que define los recursos de la pila y actualizando la pila. Para obtener más información, consulta ¿Qué es la deriva? en la Guía del CloudFormation usuario de AWS.

La respuesta de seguridad automatizada en AWS incluye el manual de correcciones para los estándares de seguridad definidos como parte de lo siguiente:

- Centro de Seguridad de Internet (CIS) AWS Foundations Benchmark v1.2.0
- Índice de referencia sobre bases de AWS de CIS, versión 1.4.0
- Índice de referencia sobre bases de AWS de CIS, versión 3.0.0
- Prácticas recomendadas de seguridad fundamentales (FSBP) de AWS v.1.0.0
- Estándar de seguridad de datos del sector de tarjetas de pago (PCI-DSS) v3.2.1
- Instituto Nacional de Estándares y Tecnología (NIST) SP 800-53 Rev. 5

La solución también incluye un manual de estrategias de controles de seguridad (SC) para la función de hallazgos de control consolidados de AWS Security Hub. Para obtener más información, consulte los manuales de estrategias.

Esta guía de implementación analiza las consideraciones arquitectónicas y los pasos de configuración para implementar la solución Automated Security Response on AWS en la nube de AWS. Incluye enlaces a CloudFormation plantillas de AWS que lanzan, configuran y ejecutan los servicios de cómputo, red, almacenamiento y otros servicios de AWS necesarios para implementar esta solución en AWS, utilizando las prácticas recomendadas de AWS en materia de seguridad y disponibilidad.

La guía está destinada a arquitectos, administradores y DevOps profesionales de infraestructuras de TI con experiencia práctica en la arquitectura en la nube de AWS.

Características y ventajas

La respuesta de seguridad automatizada de AWS ofrece las siguientes funciones:

Corrija automáticamente los hallazgos relacionados con controles específicos

Active EventBridge las reglas de Amazon para los controles para corregir automáticamente los hallazgos de ese control inmediatamente después de que aparezcan en AWS Security Hub.

Gestione las correcciones en varias cuentas y regiones desde una sola ubicación

Desde una cuenta de administrador de AWS Security Hub que esté configurada como destino de agregación para las cuentas y regiones de su organización, inicie una corrección en caso de que se encuentre en cualquier cuenta o región en la que se haya implementado la solución.

Reciba notificaciones sobre las medidas correctivas y los resultados

Suscríbase al tema Amazon SNS implementado por la solución para recibir notificaciones cuando se inicien las correcciones y si la remediación se realizó correctamente o no.

Intégrelo con sistemas de tickets como Jira o ServiceNow

Para ayudar a su organización a reaccionar ante las medidas correctivas (por ejemplo, actualizar el código de infraestructura), esta solución puede transferir los tickets a su sistema de emisión de tickets externo.

Utilice AWSConfig remediaciones en las particiones GovCloud y China

Algunas de las correcciones incluidas en la solución son repaquetes de documentos de AWSConfig remediación propiedad de AWS que están disponibles en la partición comercial, pero no en China. GovCloud Implemente esta solución para utilizar estos documentos en esas particiones.

Amplíe la solución con soluciones personalizadas e implementaciones de Playbook

La solución está diseñada para ser ampliable y personalizable. Para especificar una implementación de remediación alternativa, implemente documentos de automatización de AWS Systems Manager personalizados y funciones de IAM de AWS. Para admitir un conjunto de controles completamente nuevo que la solución no implementa, implemente un manual personalizado.

Casos de uso

Haga cumplir una norma en todas las cuentas y regiones de su organización

Implemente el manual de un estándar (por ejemplo, AWS Foundational Security Best Practices) para poder utilizar las soluciones proporcionadas. Inicie de forma automática o manual las correcciones de los recursos de cualquier cuenta o región en la que se implemente la solución para corregir los recursos que no cumplan con las normas.

Implemente soluciones personalizadas o manuales de estrategia para satisfacer las necesidades de cumplimiento de su organización

Usa los componentes de Orchestrator proporcionados como marco. Cree soluciones personalizadas para abordar out-of-compliance los recursos de acuerdo con las necesidades específicas de su organización.

Conceptos y definiciones

En esta sección se describen los conceptos clave y se define la terminología específica de esta solución:

remediación, manual de remediación

Implementación de un conjunto de pasos que resuelve un hallazgo. Por ejemplo, una solución para el control Security Control (SC) Lambda.1 «Las políticas de funciones Lambda deberían prohibir el acceso público» modificaría la política de la función Lambda de AWS correspondiente para eliminar las declaraciones que permiten el acceso público.

manual de control

Forma parte de un conjunto de documentos de automatización de AWS Systems Manager (SSM) que el orquestador utiliza para dirigir una corrección iniciada para un control específico al manual de ejecución de correcciones correcto. Por ejemplo, las correcciones de SC Lambda.1 y AWS Foundational Security Best Practices (FSBP) Lambda.1 se implementan con el mismo manual de correcciones. El Orchestrator invoca el manual de control de cada control, que se denominan ASR-AFSBP_Lambda.1 y ASR-SC_2.0.0_Lambda.1, respectivamente. Cada manual de control invoca el mismo manual de correcciones, que en este caso sería ASR-. RemoveLambdaPublicAccess

orquestador

Las Step Functions implementadas por la solución, que toman como entrada un objeto de búsqueda de AWS Security Hub e invocan el manual de control correcto en la cuenta y la región de destino. El orquestador también notifica al tema de SNS de la solución cuando se inicia la corrección y si la corrección se realiza correctamente o no.

estándar

Un grupo de controles definido por una organización como parte de un marco de cumplimiento. Por ejemplo, uno de los estándares compatibles con AWS Security Hub y esta solución es AWS FSBP.

control

Una descripción de las propiedades que un recurso debe o no debe tener para cumplir con las normas. Por ejemplo, el control AWS FSBP Lambda.1 establece que AWS Lambda Functions debe prohibir el acceso público. Una función que permita el acceso público no superaría este control.

resultados de control consolidados, control de seguridad, vista de controles de seguridad

Una función de AWS Security Hub que, cuando se activa, muestra los hallazgos con su control consolidado IDs en lugar de IDs que correspondan a un estándar en particular. Por ejemplo, los controles AWS FSBP S3.2, CIS v1.2.0 2.3, CIS v1.4.0 2.1.5.2 y PCI-DSS v3.2.1 S3.1 se asignan al control consolidado (SC) S3.2 «Los buckets S3 deben prohibir el acceso de lectura público». Cuando esta función está activada, se utilizan los manuales de instrucciones de SC.

Para obtener una referencia general de los términos de AWS, consulte el glosario de AWS.

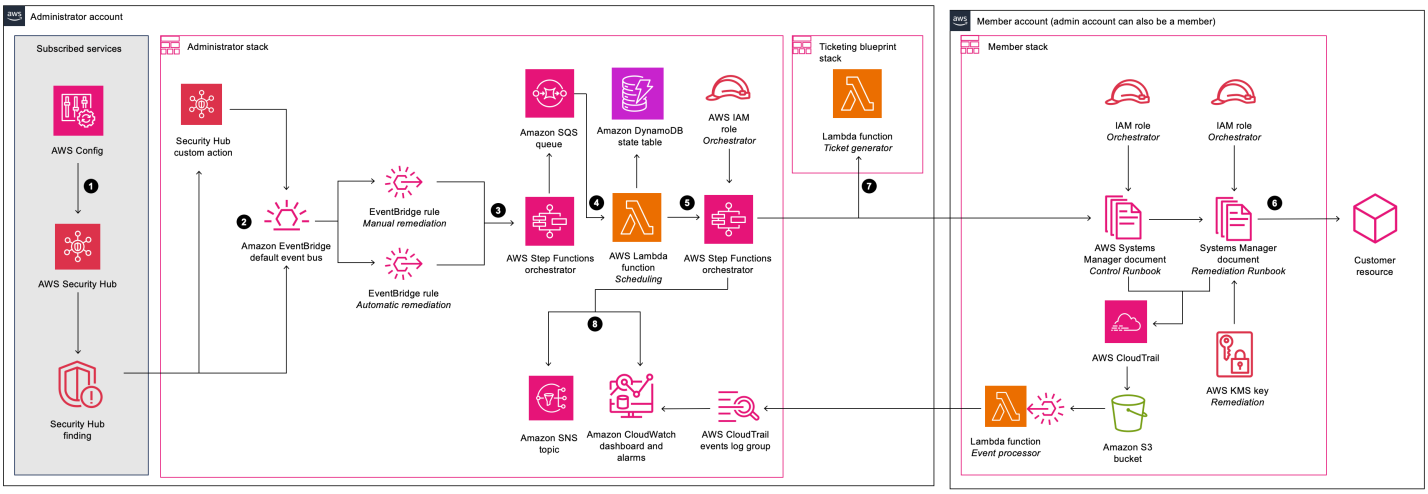
Información general de la arquitectura

En esta sección se proporciona un diagrama de arquitectura de implementación de referencia para los componentes implementados con esta solución.

Diagrama de arquitectura

Al implementar esta solución con los parámetros predeterminados, se crea el siguiente entorno en la nube de AWS.

Respuesta de seguridad automatizada en la arquitectura de AWS



> **Note**
>
> Los CloudFormation recursos de AWS se crean a partir de componentes del AWS Cloud Development Kit (AWS CDK).

El flujo de proceso de alto nivel para los componentes de la solución implementados con la CloudFormation plantilla de AWS es el siguiente:

1. Detectar: AWS Security Hub ofrece a los clientes una visión completa del estado de seguridad de AWS. Les ayuda a medir su entorno en función de los estándares y las mejores prácticas del sector de la seguridad. Funciona mediante la recopilación de eventos y datos de otros servicios de AWS, como AWS Config, Amazon Guard Duty y AWS Firewall Manager. Estos eventos y datos

se analizan en función de los estándares de seguridad, como CIS AWS Foundations Benchmark. Las excepciones se afirman como hallazgos en la consola de AWS Security Hub. Los nuevos hallazgos se envían como EventBridge eventos de Amazon.

2. Iniciar: puede iniciar eventos en función de los hallazgos mediante acciones personalizadas, que se traducen en EventBridge eventos. Las acciones y EventBridge reglas personalizadas de AWS Security Hub inician la respuesta de seguridad automatizada en los manuales de AWS para abordar los hallazgos. La solución implementa:
   a. Una EventBridge regla que coincida con el evento de acción personalizado
   b. Una regla de EventBridge evento para cada control compatible (desactivada de forma predeterminada) para que coincida con el evento de búsqueda en tiempo real

   Puede utilizar el menú de acciones personalizadas de la consola de Security Hub para iniciar la corrección automática. Tras realizar pruebas exhaustivas en un entorno que no sea de producción, también puede activar las correcciones automatizadas. Puede activar las automatizaciones para las correcciones individuales; no es necesario activar las iniciaciones automáticas en todas las correcciones.
3. Corrección previa: en la cuenta de administrador, AWS Step Functions procesa el evento de corrección y lo prepara para su programación.
4. Programación: la solución invoca la función de programación de AWS Lambda para colocar el evento de corrección en la tabla de estados de Amazon DynamoDB.
5. Orchestrate: en la cuenta de administrador, Step Functions utiliza funciones multicuentas de AWS Identity and Access Management (IAM). Step Functions invoca la corrección en la cuenta del miembro que contiene el recurso que produjo la comprobación de seguridad.
6. Corregir: un documento de automatización de AWS Systems Manager en la cuenta del miembro lleva a cabo la acción necesaria para corregir el hallazgo en el recurso de destino, como deshabilitar el acceso público de Lambda.

   Si lo desea, puede activar la función de registro de acciones en las pilas de miembros con el parámetro Log. EnableCloudTrailFor ASRAction Esta función captura las acciones que realiza la solución en tus cuentas de miembros y las muestra en el CloudWatch panel de Amazon de la solución.
7. (Opcional) Cree un ticket: si utiliza el TicketGenFunctionNameparámetro para habilitar la emisión de tickets en la pila de administración, la solución invoca la función Lambda generadora de tickets proporcionada. Esta función Lambda crea un ticket en su servicio de venta de entradas una vez que la corrección se haya ejecutado correctamente en la cuenta del miembro. Proporcionamos paquetes para la integración con Jira y. ServiceNow

8. Notificar y registrar: el manual registra los resultados en un grupo de CloudWatch registros, envía una notificación a un tema de Amazon Simple Notification Service (Amazon SNS) y actualiza los resultados del Security Hub. La solución mantiene un registro de auditoría de las acciones en las notas de los resultados.

Consideraciones sobre el diseño de AWS Well-Architected

Esta solución se diseñó con las mejores prácticas del AWS Well-Architected Framework, que ayuda a los clientes a diseñar y operar cargas de trabajo confiables, seguras, eficientes y rentables en la nube. En esta sección se describe cómo se aplicaron los principios de diseño y las mejores prácticas del Well-Architected Framework al crear esta solución.

Excelencia operativa

En esta sección se describe cómo diseñamos esta solución utilizando los principios y las prácticas recomendadas del pilar de excelencia operativa.

- Los recursos se definen como el uso de la IaC. CloudFormation
- Las medidas correctivas se implementaron con las siguientes características, siempre que fue posible:
  - Idempotencia
  - Gestión y notificación de errores
  - Registro
  - Restaurar los recursos a un estado conocido en caso de fallo

Seguridad

En esta sección se describe cómo diseñamos esta solución utilizando los principios y las prácticas recomendadas del pilar de seguridad.

- IAM utilizado para la autenticación y la autorización.
- El alcance de los permisos de rol debe ser lo más limitado posible, aunque en muchos casos esta solución requiere permisos comodín para poder actuar en cualquier recurso.

Fiabilidad

En esta sección se describe cómo diseñamos esta solución utilizando los principios y las prácticas recomendadas del pilar de fiabilidad.

- Security Hub continúa creando hallazgos si la remediación no resuelve la causa subyacente del hallazgo.
- Los servicios sin servidor permiten escalar la solución según sea necesario.

Eficiencia del rendimiento

En esta sección se describe cómo diseñamos esta solución utilizando los principios y las prácticas recomendadas del pilar de eficiencia del rendimiento.

- Esta solución se diseñó para ser una plataforma que pueda ampliarse sin tener que implementar usted mismo la organización y los permisos.

Optimización de costos

En esta sección se describe cómo diseñamos esta solución utilizando los principios y las prácticas recomendadas del pilar de optimización de costos.

- Los servicios sin servidor le permiten pagar sólo por lo que utiliza.
- Utilice la capa gratuita para la automatización de SSM en todas las cuentas

Sostenibilidad

En esta sección se describe cómo diseñamos esta solución utilizando los principios y las mejores prácticas del pilar de sostenibilidad.

- Los servicios sin servidor permiten escalar verticalmente u horizontalmente la solución según sea necesario.

Detalles de la arquitectura

En esta sección se describen los componentes y los servicios de AWS que componen esta solución y los detalles de la arquitectura sobre cómo funcionan juntos estos componentes.

Integración de AWS Security Hub

La implementación de la `automated-security-response-admin` pila crea una integración con la función de acción personalizada de AWS Security Hub. Cuando los usuarios de la consola AWS Security Hub seleccionan Findings para su corrección, la solución distribuye el registro de búsqueda para su corrección mediante AWS Step Functions.

Los permisos entre cuentas y los manuales de ejecución de AWS Systems Manager deben implementarse en todas las cuentas de AWS Security Hub (administrador y miembro) mediante las plantillas `automated-security-response-member.template` y `automated-security-response-member-roles.template` CloudFormation . Para obtener más información, consulte los manuales de estrategias. Esta plantilla permite la corrección automática en la cuenta de destino.

Los usuarios pueden iniciar automáticamente soluciones automatizadas para cada remediación mediante las reglas de eventos de Amazon CloudWatch . Esta opción activa la corrección totalmente automática de los hallazgos en cuanto se notifican a AWS Security Hub. De forma predeterminada, las iniciaciones automáticas están desactivadas. Esta opción se puede cambiar en cualquier momento durante o después de la instalación del manual activando las reglas de CloudWatch eventos en la cuenta de administrador de AWS Security Hub.

Solución de problemas entre cuentas

Automated Security Response en AWS utiliza funciones entre cuentas para funcionar en cuentas principales y secundarias mediante funciones entre cuentas. Estas funciones se implementan en las cuentas de los miembros durante la instalación de la solución. A cada corrección se le asigna una función individual. Al proceso de corrección de la cuenta principal se le concede permiso para asumir la función de corrección en la cuenta que requiere la corrección. La corrección la llevan a cabo los runbooks de AWS Systems Manager que se ejecutan en la cuenta que requiere la corrección.

Libros de jugadas

Un conjunto de soluciones se agrupa en un paquete denominado manual de estrategias. Los libros de estrategias se instalan, actualizan y eliminan mediante las plantillas de esta solución. Para obtener información sobre las soluciones compatibles en cada libro de jugadas, consulte la Guía para desarrolladores → Guías de estrategias. Actualmente, esta solución es compatible con los siguientes manuales de estrategias:

- Security Control, un manual alineado con la función de hallazgos de control consolidados de AWS Security Hub, publicado el 23 de febrero de 2023.

  > **Important**
  >
  > Cuando los hallazgos de control consolidados están habilitados en Security Hub, este es el único manual que debe habilitarse en la solución.

- Análisis comparativos de Amazon Web Services Foundations del Center for Internet Security (CIS), versión 1.2.0, publicados el 18 de mayo de 2018.
- Puntos de referencia de Amazon Web Services Foundations del Center for Internet Security (CIS), versión 1.4.0, publicados el 9 de noviembre de 2022.
- Puntos de referencia de Amazon Web Services Foundations del Center for Internet Security (CIS), versión 3.0.0, publicados el 13 de mayo de 2024.
- AWS Foundational Security Best Practices (FSBP) versión 1.0.0, publicada en marzo de 2021.
- Los estándares de seguridad de datos del sector de las tarjetas de pago (PCI-DSS), versión 3.2.1, publicados en mayo de 2018.
- Versión 5.0.0 del Instituto Nacional de Estándares y Tecnología (NIST), publicada en noviembre de 2023.

Registro centralizado

La respuesta de seguridad automatizada en AWS registra en un único grupo de CloudWatch registros, SO0111-ASR. Estos registros contienen registros detallados de la solución para la resolución de problemas y la administración de la solución.

Notificaciones

Esta solución utiliza un tema del Amazon Simple Notification Service (Amazon SNS) para publicar los resultados de las correcciones. Puede utilizar las suscripciones a este tema para ampliar las capacidades de la solución. Por ejemplo, puede enviar notificaciones por correo electrónico y actualizar los tickets de problemas.

- SO0111-ASR_topic: se utiliza para enviar información general y mensajes de error relacionados con las correcciones ejecutadas.
- SO0111-ASR_Alarm_Topic: se utiliza para notificar cuando se activa una de las alarmas de la solución, lo que indica que la solución no funciona como se esperaba.

Los servicios de AWS en esta solución

La solución utiliza los siguientes servicios. Los servicios principales son necesarios para usar la solución y los servicios de soporte conectan los servicios principales.

Servicio de AWS	Descripción
Amazon EventBridge	Principal. Despliega eventos que iniciarán la función escalonada del orquestador cuando se corrija un hallazgo.
AWS IAM	Principal. Despliega muchas funciones para permitir la corrección de problemas en distintos recursos.
AWS Lambda	Principal. Implementa varias funciones lambda que utilizará el orquestador de funciones escalonadas para solucionar problemas.
AWS Security Hub	Principal. Ofrece a los clientes una visión completa del estado de seguridad de AWS.
AWS Step Functions	Principal. Implementa un orquestador que invocará los documentos de corrección con las llamadas a la API de AWS Systems Manager.

Servicio de AWS	Descripción
AWS Systems Manager	Principal. Implementa los documentos del administrador del sistema (enlace al documento) que contienen la lógica de corrección que se ejecutará.
AWS CloudTrail	Admite. Registra los cambios que la solución realiza en sus recursos de AWS y los muestra en un CloudWatch panel de control.
Amazon CloudWatch	Admite. Implementa grupos de registros que los distintos manuales de estrategias utilizarán para registrar los resultados. Recopila métricas para mostrarlas en un panel personalizado con alarmas.
AWS DynamoDB	Admite. Almacena la última corrección ejecutada en cada cuenta y región para optimizar la programación de las correcciones.
Amazon Simple Notification Service	Admite. Despliega los temas de SNS que reciben una notificación una vez que se ha completado la corrección.
AWS SQS	Admite. Ayuda a programar las correcciones para que la solución pueda ejecutarlas en paralelo.
AWS Key Management Service	Admite. Se utiliza para cifrar los datos con fines de remediación.
AWS Config	Admite. Registra todos los recursos para usarlos con AWS Security Hub.

Planificación de la implementación

En esta sección se describen el costo, la seguridad de la red, las regiones de AWS compatibles, las cuotas y otras consideraciones antes de implementar la solución.

Costo

Usted es responsable del coste de los servicios de AWS utilizados para ejecutar esta solución.

A partir de esta revisión, los costos mensuales estimados son:

- Implementación pequeña (10 cuentas, 1 región: EE. UU. East/N. Virginia): Approximately $21.17 for 300 remediations/month
- Despliegue medio (100 cuentas, 1 región: EE. UU. East/N. Virginia): Approximately $134.86 for 3,000 remediations/month
- Implementación de gran tamaño (1 000 cuentas, 10 regiones): aproximadamente 10 271,70$ para 30 000 reparaciones al mes

> **Important**
>
> Los precios están sujetos a cambios. Para obtener más información, consulte la página de precios de cada servicio de AWS utilizado en esta solución.

> **Note**
>
> Muchos servicios de AWS incluyen una capa gratuita, un importe básico del servicio que los clientes pueden utilizar sin coste alguno. Los costos reales pueden ser superiores o inferiores a los de los ejemplos de precios proporcionados.

Recomendamos crear un presupuesto a través de AWS Cost Explorer para ayudar a administrar los costos. Los precios están sujetos a cambios. Para obtener más información, consulte la página web de precios de cada servicio de AWS utilizado en esta solución.

Ejemplo de tabla de costos

El costo total de ejecutar esta solución depende de los siguientes factores:

- Número de cuentas de miembros de AWS Security Hub
- El número de correcciones activas que se invocan automáticamente
- La frecuencia de las correcciones

Esta solución utiliza los siguientes componentes de AWS, que conllevan un coste en función de la configuración. Se proporcionan ejemplos de precios para organizaciones pequeñas, medianas y grandes.

Servicio	Capa gratuita	Precios [USD]
AWS Systems Manager Automation: recuento de pasos	100 000 pasos por cuenta al mes	Más allá del nivel gratuito, cada paso básico tiene un coste de 0,002$ por paso. En el caso de las automatiz aciones con varias cuentas, todos los pasos, incluidos los realizados en cualquier cuenta secundaria, se contabilizan únicamente en la cuenta de origen.
AWS Systems Manager Automation: duración del paso	5000 segundos al mes	Más allá del nivel gratuito, cada paso de acción de AWS:ExecuteScript cuesta 0,00003$ por segundo, después del nivel gratuito de 5000 segundos al mes.
AWS Systems Manager Automation - Almacenamiento	No hay capa gratuita	0,046$ por GB al mes

Servicio	Capa gratuita	Precios [USD]
AWS Systems Manager Automation: Transferencia de datos	No hay capa gratuita	0,900 USD por GB transferido (para cuentas múltiples o) out-of-Region
AWS Security Hub: Comprobaciones de seguridad	No hay un nivel gratuito	Los primeros 100.000 dólares checks/account/Region/month cuestan 0,0010$ por cheque Los siguientes 400 000 dólares checks/account/Region/month cuestan 0,0008 dólares por cheque Más de 500 000 dólares checks/account/Region/month cuestan 0,0005$ por cheque
AWS Security Hub: Búsqueda de eventos de ingestión	Los primeros 10 000 puntos events/account/Region/month son gratuitos. Búsqueda de eventos de ingestión asociados a las comprobaciones de seguridad de Security Hub.	Más de 10 000€ events/account/Region/month cuestan 0,00003$ por evento

Servicio	Capa gratuita	Precios [USD]
Amazon CloudWatch : métricas	Métricas de monitoreo básicas (con una frecuencia de 5 minutos) 10 métricas de monitoreo detalladas (con una frecuencia de 1 minuto) 1 millón de solicitudes de API (no se aplica a GetMetricData y GetMetricWidgetImage)	Las primeras 10 000 métricas cuestan 0,30$ por métrica al mes Las siguientes 240.000 métricas cuestan 0,10$ por métrica al mes Las siguientes 750 000 métricas cuestan 0,05$ por métrica al mes Más de 1 000 000 de métricas cuestan 0,02$ por métrica al mes Las llamadas a la API cuestan 0,01$ por cada 1000 solicitudes
Amazon CloudWatch - Panel de control	3 paneles de control para un máximo de 50 métricas al mes	3,00$ por panel de control al mes

Servicio	Capa gratuita	Precios [USD]
Amazon CloudWatch - Alarmas	10 métricas de alarma (no aplicables a las alarmas de alta resolución)	La resolución estándar (60 segundos) cuesta 0,10 USD por alarma La alta resolución (10 segundos) cuesta 0,30$ por métrica de alarma La detección de anomalías con resolución estándar cuesta 0,30$ por alarma La detección de anomalías de alta resolución cuesta 0,90$ por alarma La tecnología compuesta cuesta 0,50$ por alarma
Amazon CloudWatch - Colección de registros	5 GB de datos (ingestión, almacenamiento de archivos y datos escaneados mediante consultas de Logs Insights)	0,50 USD por GB
Amazon CloudWatch - Almacenamiento de registros	5 GB de datos (ingestión, almacenamiento de archivos y datos escaneados mediante consultas de Logs Insights)	0,005 USD por GB de datos escaneados
Amazon CloudWatch - Eventos	Se incluyen todos los eventos excepto los eventos personali zados	1,00$ por millón de eventos para eventos personalizados, 1,00$ por millón de eventos para eventos multicuenta
AWS Lambda: Solicitudes	1 millón de solicitudes gratuitas al mes	0,20$ por 1 millón de solicitud es

Servicio	Capa gratuita	Precios [USD]
AWS Lambda: duración	400 000 GB-segundos de tiempo de cómputo al mes	0,0000166667$ por cada GB por segundo. El precio de la duración depende de la cantidad de memoria que asignes a la función. Puedes asignar cualquier cantidad de memoria a tu función, entre 128 MB y 10 240 MB, en incrementos de 1 MB.
AWS Step Functions: Transiciones de estado	4000 transiciones de estado gratuitas al mes	A partir de entonces, 0,025 USD por cada 1000 estados
Amazon EventBridge	Todos los eventos de cambio de estado publicados por los servicios de AWS son gratuitos	Los eventos personalizados cuestan 1 dólar por millón de dólares. La publicación de eventos personalizados Los eventos de terceros (SaaS) cuestan 1 dólar por millón de dólares. Los eventos publicados El envío de eventos multicuenta cuesta 1 dólar por millón de dólares
Amazon SNS	El primer millón de solicitudes de Amazon SNS al mes son gratuitas	A partir de entonces, 0,50 USD por cada millón de solicitudes
Amazon SQS	El primer millón de solicitudes de Amazon SQS al mes son gratuitas	A partir de entonces, 0,40 USD por millón y 100 000 millones de solicitudes

Servicio	Capa gratuita	Precios [USD]
Amazon DynamoDB	Los primeros 25 GB de almacenamiento son gratuitos	2,00$ por cada millón de lecturas y escrituras consistentes a partir de entonces
Precios de AWS Key Management Service	20 000 solicitudes al mes	1,00$ por clave de 1 KMS. En el caso de las claves KMS que se rotan automáticamente o a pedido, la primera y la segunda rotación de la clave añaden un dólar al mes (prorrateado por hora) de coste.

Ejemplos de precios (mensuales)

Ejemplo 1:300 correcciones al mes

- 10 cuentas, 1 región
- 30 remediaciones por account/Region/month
- El costo total es de 21,17$ al mes

Servicio	Supuestos	Cargos mensuales [USD]
Automatización de AWS Systems Manager	Pasos: aproximadamente 4 pasos* 300 soluciones * 0,002$ = 2,40$ Duración: 10 segundos * 300 soluciones * 0,00003$ = 0,09$	2,49$
AWS Security Hub	No se utilizaron servicios facturables	$0

Servicio	Supuestos	Cargos mensuales [USD]
Amazon CloudWatch Logs	300 soluciones * 0,000002$ = 0,0006$ 0,0006$ * 0,03 = 0,000018$	< 0,01$
AWS Lambda: Solicitudes	300 soluciones * 6 solicitudes = 1800 solicitudes 0,20$ * 1 000 000 de solicitudes = 0,20$	0,20$
AWS Lambda: duración	256 millones: 1,875 GB por segundo * 300 correcciones * 0,0000167$ = 0,009375$	< 0,01$
AWS Step Functions	17 transiciones de estado * 300 remediaciones = 5.100 0,025 USD* (5.100/1.000) transiciones de estado = 0,15$	0,15$
EventBridge Reglas de Amazon	Las reglas no cobran	$0
AWS Key Management Service	1 clave * 10 cuentas * 1 región * 1 dólar = 10$	10,00$
Amazon DynamoDB	2,00$ * 1 000 000 000$ de lectura y escritura = 2,00$	2,00$
Amazon SQS	0,40$ * 1 000 000 de solicitudes = 0,40$	0,40$
Amazon SNS	0,50$ * 1 000 000 000 de notificaciones = 0,50$	0,50$

Servicio	Supuestos	Cargos mensuales [USD]
Amazon CloudWatch : métricas	0,30$ * 7 métricas personalizadas = 2,10$ 0,01 USD * (300 x 3/1000) llamadas a la API con métricas de venta = 0,01 USD	2,11$
Amazon CloudWatch : paneles de control	3,00$ * 1 panel = 3,00$	3,00$
Amazon CloudWatch - Alarmas	0,10$ * 3 alarmas = 0,30$	0,30$
Total		21,17 DÓLARES

Ejemplo 2:3000 reparaciones al mes

- 100 cuentas, 1 región
- 30 remediaciones por account/Region/month
- Coste total de 134,86$ al mes

Servicio	Supuestos	Cargos mensuales [USD]
Automatización de AWS Systems Manager	Pasos: aproximadamente 4 pasos* 3000 remediaciones * 0,002$ = 24,00$ Duración: 10 segundos * 3000 remediaciones * 0,00003$ = 0,90$	24,90$
AWS Security Hub	No se utilizaron servicios facturables	$0

Servicio	Supuestos	Cargos mensuales [USD]
Amazon CloudWatch Logs	3000 soluciones * 0,000002$ = 0,006$ 0,006$ * 0,03 = 0,00018$	< 0,01$
AWS Lambda: Solicitudes	3000 correcciones * 6 solicitudes = 18 000 solicitudes 0,20$ * 1 000 000 de solicitudes = 0,20$	0,20$
AWS Lambda: duración	256 millones: 1,875 GB por segundo * 3000 correcciones * 0,000167$ = 0,09375$	0,09$
AWS Step Functions	17 transiciones entre estados * 3000 remediaciones = 51 000 0,025 dólares* (51.000/1.000) transiciones de estado = 1,275$	1,28$
EventBridge Reglas de Amazon	Las reglas no cobran	$0
AWS Key Management Service	1 clave * 100 cuentas * 1 región * 1 dólar = 100$	100 USD
Amazon DynamoDB	2,00$ * 1 000 000$ de lectura y escritura = 2,00$	2,00$
Amazon SQS	0,40$ * 1 000 000 de solicitudes = 0,40$	0,40$
Amazon SNS	0,50$ * 1 000 000 000 de notificaciones = 0,50$	0,50$

Servicio	Supuestos	Cargos mensuales [USD]
Amazon CloudWatch : métricas	0,30$ * 7 métricas personalizadas = 2,10$ 0,01 USD * (3000 x 3/1000) llamadas a la API con métricas de venta = 0,09 USD	2,19$
Amazon CloudWatch : paneles de control	3,00$ * 1 panel = 3,00$	3,00$
Amazon CloudWatch - Alarmas	0,10$ * 3 alarmas = 0,30$	0,30$
Total		134,86 DÓLARES

Ejemplo 3:30 000 reparaciones al mes

- 1000 cuentas, 10 regiones
- 30 soluciones por account/Region/month
- El costo total es de 1.271,70$ al mes

Servicio	Supuestos	Cargos mensuales [USD]
Automatización de AWS Systems Manager	Pasos: aproximadamente 4 pasos* 30 000 soluciones * 0,002$ = 240,00$ Duración: 10 segundos * 30 000 soluciones * 0,00003$ = 9,00$	249,00$
AWS Security Hub	No se utilizaron servicios facturables	$0

Servicio	Supuestos	Cargos mensuales [USD]
Amazon CloudWatch Logs	30 000 soluciones * 0,000002$ = 0,06$ 0,06 USD * 0,03 = 0,0018 USD	< 0,01$
AWS Lambda: Solicitudes	30 000 correcciones * 6 solicitudes = 180 000 solicitudes 0,20$ * 1 000 000 de solicitudes = 0,20$	0,20$
AWS Lambda: duración	256 millones: 1,875 GB por segundo * 30 000 correcciones * 0,000167$ = 0,9375$	0,94$
AWS Step Functions	17 transiciones entre estados * 30 000 correcciones = 510 000 0,025 USD * (510 000/1000) transiciones de estado = 12,75 USD	12,75$
EventBridge Reglas de Amazon	Las reglas no cobran	$0
AWS Key Management Service	(1 clave) 1 dólar * 1000 cuentas * 10 regiones = 10 000$	10.000$
Amazon DynamoDB	0,000002 dólares* 1 000 000$ de lectura y escritura = 2,00$	2,00$
Amazon SQS	0,000004 dólares* 1 000 000 de solicitudes = 0,40$	0,40$

Servicio	Supuestos	Cargos mensuales [USD]
Amazon SNS	0,000005 dólares* 1 000 000 de notificaciones = 0,50$	0,50$
Amazon CloudWatch : métricas	0,30$ * 6 métricas personalizadas = 1,80$ 0,01 USD * (30 000 x 3/1000) llamadas a la API con métricas de venta = 0,90 USD	2,70$
Amazon CloudWatch : paneles de control	3,00$ * 1 panel = 3,00$	3,00$
Amazon CloudWatch - Alarmas	0,10$ * 2 alarmas = 0,20$	0,20$
Total		10.271,70 DÓLARES

Important

Costos de rotación de claves de KMS: AWS Key Management Service (KMS) rota automáticamente las claves administradas por el cliente una vez al año cuando la rotación está habilitada. Cada rotación conlleva un coste de 1 dólar por clave al año. Por ejemplo, con 1000 cuentas en una sola región, esto se traduce en 1000$ adicionales al año (1 rotación × 1000 claves × 1,00$).

Coste adicional por las funciones opcionales

En esta sección, se indican los costos adicionales asociados a las funciones opcionales de esta solución.

CloudWatch Métricas mejoradas

Si selecciona `yes` el EnableEnhancedCloudWatchMetricsparámetro al implementar la pila de administración, la solución crea dos métricas personalizadas y una alarma para cada ID de control.

El costo depende de la cantidad de controles IDs que vaya a corregir. En la siguiente tabla, se supone que se corrigen los 96 controles diferentes IDs al mes para determinar el límite superior de los costes.

Servicio	Supuestos: 96 controles IDs * 2 = 192 métricas personalizadas	Cargos mensuales [USD]
Amazon CloudWatch : métricas	0,30$ * 192 métricas personalizadas = 57,60$	57,60$
Amazon CloudWatch - Alarmas	0,10$ * 96 alarmas = 9,60$	9,60$
Total		67,20 DÓLARES

CloudTrail Registro de acciones

En cada cuenta de miembro en la que se habilita la función de registro de acciones, la solución crea un registro CloudTrail para registrar todos los eventos de administración de escritura. Una función Lambda filtra los eventos no relacionados con la solución. Esto significa que el costo está relacionado con la cantidad total de eventos de administración de su cuenta, ya que los eventos que no están relacionados con la solución siguen siendo capturados por el registro y procesados por la función Lambda.

Para la siguiente tabla, suponemos que hay 150 000 eventos de gestión al mes en la cuenta. El coste real depende de la actividad real de los eventos de gestión en su cuenta.

Servicio	Supuestos	Cargos mensuales [USD]
AWS CloudTrail	150.000 * 2,00 USD/100 000 = 3,00$	3,00$
Lambda	150.000 x 0,2 x 0,125 = 3.750 GB-segundos	0,0925$

Servicio	Supuestos	Cargos mensuales [USD]
	3.750$ * 0,0000166667$ = 0,0625$ de coste de tiempo de cálculo 0,15 * 0,20$ = 0,03$ de coste de solicitud 0,0625$ + 0,03$ = 0,0952$ de coste total de Lambda	
Total		3,09$ por cuenta de miembro

Seguridad

Cuando crea sistemas en la infraestructura de AWS, las responsabilidades de seguridad se comparten entre usted y AWS. Este modelo compartido reduce la carga operativa porque AWS opera, administra y controla los componentes, incluidos el sistema operativo anfitrión, la capa de virtualización y la seguridad física de las instalaciones en las que operan los servicios. Para obtener más información sobre la seguridad de AWS, visite AWS Cloud Security.

Roles de IAM

Las funciones de AWS Identity and Access Management (IAM) permiten a los clientes asignar políticas y permisos de acceso detallados a los servicios y usuarios de la nube de AWS. Esta solución crea funciones de IAM que otorgan a las funciones automatizadas de la solución acceso para realizar acciones de remediación dentro de un conjunto limitado de permisos específicos para cada remediación.

La función Step de la cuenta de administrador está asignada a la función SO0111-. ASR-Orchestrator-Admin Solo este rol puede asumir el rol de miembro del SO0111 Orchestrator en cada cuenta de miembro. Cada función de remediación permite que el rol de miembro lo transfiera al servicio AWS Systems Manager para ejecutar manuales de remediación específicos. Los nombres de los roles de remediación comienzan por SO0111, seguidos de una descripción que coincide con el nombre del manual de remediación. Por ejemplo, SO0111-Remove es la función del manual de correcciones de ASR-Remove VPCDefaultSecurityGroupRules . VPCDefault SecurityGroupRules

Regiones de AWS admitidas

Nombre de región	Código de región
Este de EE. UU. (Ohio)	us-east-2
Este de EE. UU. (Norte de Virginia)	us-east-1
EE.UU. Oeste (Norte de California)	us-west-1
Oeste de EE. UU. (Oregón)	us-west-2
África (Ciudad del Cabo)	af-south-1
Asia-Pacífico (Hong Kong)	ap-east-1
Asia-Pacífico (Hyderabad)	ap-south-2
Asia-Pacífico (Yakarta)	ap-southeast-3
Asia-Pacífico (Melbourne)	ap-southeast-4
Asia-Pacífico (Bombay)	ap-south-1
Asia-Pacífico (Osaka)	ap-northeast-3
Asia-Pacífico (Seúl)	ap-northeast-2
Asia-Pacífico (Singapur)	ap-southeast-1
Asia-Pacífico (Sídney)	ap-southeast-2
Asia-Pacífico (Tokio)	ap-northeast-1
Canadá (centro)	ca-central-1
Europa (Fráncfort)	eu-central-1
Europa (Irlanda)	eu-west-1
Europa (Londres)	eu-west-2

Nombre de región	Código de región
Europa (Milán)	eu-south-1
Europa (París)	eu-west-3
Europa (España)	eu-south-2
Europa (Estocolmo)	eu-north-1
Europa (Zúrich)	eu-central-2
Medio Oriente (Baréin)	me-south-1
Medio Oriente (EAU)	me-central-1
América del Sur (São Paulo)	sa-east-1
AWS GovCloud (EE. UU. Este)	us-gov-east-1
AWS GovCloud (EE. UU. Oeste)	us-gov-west-1
China (Pekín)	cn-north-1
China (Ningxia)	cn-northwest-1
Israel (Tel Aviv)	il-central-1
Oeste de Canadá (Calgary)	ca-west-1
México (Ciudad de México)	mx-central-1
Asia-Pacífico (Tailandia)	ap-southeast-7

Note

Es posible que cualquier región nueva de AWS que no aparezca en la lista se admita mediante la implementación local, pero no mediante la implementación con un solo clic.

Cuotas

Las cuotas de servicio (que también se denominan límites) establecen el número máximo de recursos u operaciones de servicio para su cuenta de AWS.

Cuotas para los servicios de AWS en esta solución

Asegúrese de tener una cuota suficiente para cada uno de los servicios implementados en esta solución. Para obtener más información, consulte las cuotas de servicio de AWS.

Utilice los siguientes enlaces para ir a la página de ese servicio. Para ver las cuotas de servicio de todos los servicios de AWS en la documentación sin cambiar de página, consulte la información en la página de puntos finales y cuotas del servicio en el PDF.

CloudFormation Cuotas de AWS

Su cuenta de AWS tiene CloudFormation cuotas de AWS que debe tener en cuenta al lanzar la pila de esta solución. Si comprende estas cuotas, puede evitar errores de limitación que le impidan implementar esta solución correctamente. Para obtener más información, consulte CloudFormation las cuotas de AWS en la Guía del CloudFormation usuario de AWS.

CloudWatch Cuotas de AWS

Su cuenta de AWS tiene CloudWatch cuotas de AWS vinculadas a las políticas de CloudWatch recursos, que solo permiten 10 políticas de recursos por región y cuenta, y esto no se puede solicitar para un aumento de cuota; consulte AWS CloudWatch Logs Quotas en la Guía del CloudWatch usuario de AWS. Antes de la implementación, compruebe su uso actual para asegurarse de no sobrepasar este límite al implementar la solución.

Amazon EventBridge regula las cuotas

Su cuenta de AWS tiene cuotas EventBridge reglamentarias de Amazon que debe tener en cuenta a la hora de seleccionar las estrategias que desee implementar con la solución. Cada manual de estrategias creará una EventBridge regla para cada control que pueda corregir. Al implementar varios libros de jugadas, es posible alcanzar la cuota de reglas. Para obtener más información, consulta EventBridge las cuotas de Amazon en la Guía del EventBridge usuario de Amazon.

Implementación de AWS Security Hub

La implementación y la configuración de AWS Security Hub son requisitos previos para esta solución. Para obtener más información sobre la configuración del AWS Security Hub, consulte Configuración del AWS Security Hub en la Guía del usuario del AWS Security Hub.

Como mínimo, debes tener configurado un Security Hub en funcionamiento en tu cuenta principal. Puede implementar esta solución en la misma cuenta (y región de AWS) que la cuenta principal de Security Hub. En cada cuenta principal y secundaria de Security Hub, también debe implementar la plantilla de miembros que otorga AssumeRole permisos a las AWS Step Functions de la solución para ejecutar manuales de corrección en la cuenta.

Compilación frente a implementación StackSets

Un conjunto de pilas le permite crear pilas en las cuentas de AWS de todas las regiones de AWS mediante una única CloudFormation plantilla de AWS. A partir de la versión 1.4, esta solución admite la implementación de conjuntos apilados al dividir los recursos en función del lugar y la forma en que se implementan. Los clientes con varias cuentas, especialmente los que utilizan AWS Organizations, pueden beneficiarse del uso de conjuntos de pilas para la implementación en muchas cuentas. Reduce el esfuerzo necesario para instalar y mantener la solución. Para obtener más información StackSets, consulte Uso de AWS CloudFormation StackSets.

Implementación de la solución

> **Important**
>
> Si la función de hallazgos de control consolidados está activada en Security Hub (es la opción predeterminada en las nuevas implementaciones), habilite únicamente el manual de estrategias de Control de Seguridad (CS) al implementar esta solución. Si la función no está activada, habilite únicamente los manuales de estrategias para los estándares de seguridad que estén habilitados en Security Hub. Si se habilitan libros de jugadas adicionales, se puede alcanzar la cuota de EventBridge reglas.

Esta solución utiliza CloudFormation plantillas y pilas de AWS para automatizar su implementación. Las CloudFormation plantillas especifican los recursos de AWS incluidos en esta solución y sus propiedades. La CloudFormation pila aprovisiona los recursos que se describen en las plantillas.

Para que la solución funcione, se deben implementar tres plantillas. Primero, decida dónde implementar las plantillas y, a continuación, cómo implementarlas.

Esta descripción general describirá las plantillas y cómo decidir dónde y cómo implementarlas. Las siguientes secciones incluirán instrucciones más detalladas para implementar cada pila como una pila o StackSet.

Decidir dónde implementar cada pila

Las tres plantillas se denominarán con los siguientes nombres y contendrán los siguientes recursos:

- Pila de administración: función de pasos del orquestador, reglas de eventos y acción personalizada de Security Hub.
- Pila de miembros: documentos de remediación de SSM Automation.
- Pila de funciones de los miembros: funciones de IAM para las correcciones.

La pila de administradores debe implementarse una vez, en una sola cuenta y en una sola región. Debe implementarse en la cuenta y la región que haya configurado como destino de agregación para las conclusiones de Security Hub para su organización. Si desea utilizar la función de registro de

acciones para supervisar los eventos de administración, debe implementar la pila de administración en la cuenta de administración de su organización o en una cuenta de administrador delegado.

La solución funciona con los hallazgos de Security Hub, por lo que no podrá operar con los hallazgos de una cuenta o región en particular si esa cuenta o región no se ha configurado para agregar los hallazgos en la cuenta y región del administrador del Security Hub.

Por ejemplo, una organización tiene cuentas que operan en las regiones `us-east-1` y`us-west-2`, con la cuenta `111111111111` de administrador delegado del Security Hub en la regió`us-east-1`. Cuentas `222222222222` y `333333333333` deben ser cuentas de miembro de Security Hub para la cuenta `111111111111` de administrador delegado. Las tres cuentas deben estar configuradas para agregar los resultados de `us-west-2` a`us-east-1`. La pila de administración debe implementarse `111111111111` en la cuenta`us-east-1`.

Para obtener más información sobre cómo encontrar la agregación, consulte la documentación sobre las cuentas de administrador delegado de Security Hub y la agregación entre regiones.

La pila de administradores debe completar primero la implementación antes de implementar las pilas de miembros para poder crear una relación de confianza entre las cuentas de los miembros y la cuenta central.

El grupo de miembros debe implementarse en todas las cuentas y regiones en las que desees corregir los problemas. Esto puede incluir la cuenta de administrador delegado de Security Hub en la que anteriormente se implementó la pila de administración de ASR. Los documentos de automatización deben ejecutarse en las cuentas de los miembros para poder utilizar la capa gratuita de SSM Automation.

Siguiendo el ejemplo anterior, si quiere corregir los problemas de todas las cuentas y regiones, la pila de miembros debe estar desplegada en las tres cuentas (`111111111111222222222222`, y`333333333333`) y en ambas regiones (y). `us-east-1` `us-west-2`

La pila de funciones de los miembros se debe implementar en todas las cuentas, pero contiene recursos globales (funciones de IAM) que solo se pueden implementar una vez por cuenta. No importa en qué región se despliegue la pila de funciones de los miembros, por lo que, por motivos de simplicidad, le sugerimos que la despliegue en la misma región en la que se despliega la pila de funciones de administrador.

Siguiendo el ejemplo anterior, te sugerimos implementar la pila de roles de los miembros en las tres cuentas (`111111111111222222222222`, y`333333333333`)`us-east-1`.

Decidir cómo implementar cada pila

Las opciones para implementar una pila son

- CloudFormation StackSet (permisos autogestionados)
- CloudFormation StackSet (permisos administrados por el servicio)
- CloudFormation Pila

StackSets con los permisos gestionados por el servicio, son los más prácticos, ya que no requieren el despliegue de funciones propias y se pueden implementar automáticamente en las nuevas cuentas de la organización. Lamentablemente, este método no admite pilas anidadas, que utilizamos tanto en la pila de administradores como en la pila de miembros. La única pila que se puede implementar de esta manera es la pila de roles de los miembros.

Tenga en cuenta que cuando se implementa en toda la organización, la cuenta de administración de la organización no está incluida, por lo que si desea corregir los errores en la cuenta de administración de la organización, debe realizar la implementación en esta cuenta por separado.

La pila de miembros se debe implementar en todas las cuentas y regiones, pero no se puede implementar StackSets con permisos gestionados por el servicio porque contiene pilas anidadas. Por lo tanto, sugerimos implementar esta pila con StackSets permisos autogestionados.

La pila de administración solo se implementa una vez, por lo que se puede implementar como una CloudFormation pila simple o StackSet con permisos autogestionados en una sola cuenta y región.

Resultados de control consolidados

Las cuentas de su organización se pueden configurar con la función de hallazgos de control consolidados de Security Hub activada o desactivada. Consulte los resultados del control consolidado en la Guía del usuario de AWS Security Hub.

> **Important**
>
> Si está habilitada, debe usar la versión 2.0.0 de la solución o una versión posterior. Además, debe implementar las pilas agrupadas de administradores y miembros para los estándares «SC» o «control de seguridad». De este modo, se despliegan los documentos y EventBridge las reglas de automatización para utilizarlos con el control consolidado que se IDs genera al activar esta función. No es necesario implementar las pilas anidadas de administradores

o miembros para estándares específicos (por ejemplo, AWS FSBP) cuando se utiliza esta función.

CloudFormation Plantillas de AWS

View template

automa

security-response-admin.template: utilice esta plantilla para lanzar la solución Automated Security Response on AWS. La plantilla instala los componentes principales de la solución, una pila anidada para los registros de AWS Step Functions y una pila anidada para cada estándar de seguridad que decida activar.

Los servicios utilizados incluyen Amazon Simple Notification Service, AWS Key Management Service, AWS Identity and Access Management, AWS Lambda, AWS Step Functions, Amazon CloudWatch Logs, Amazon S3 y AWS Systems Manager.

Soporte para cuentas de administrador

Las siguientes plantillas se instalan en la cuenta de administrador de AWS Security Hub para activar los estándares de seguridad que desea admitir. Puede elegir cuál de las siguientes plantillas desea instalar al instalar la`automated-security-response-admin.template`.

automated-security-response-orchestrator-log.template: crea un grupo de CloudWatch registros para la función Orchestrator Step.

AFSBPStack.template: reglas de prácticas recomendadas de seguridad fundamentales de AWS v1.0.0.

CIS120stack.template: puntos de referencia de los Fundamentos de Amazon Web Services de la CEI, reglas v1.2.0.

CIS140stack.template: puntos de referencia de los Fundamentos de Amazon Web Services de la CEI, reglas v1.4.0.

CIS300stack.template: puntos de referencia de los Fundamentos de Amazon Web Services de la CEI, reglas de la versión 3.0.0.

PCI321Stack.template: reglas de PCI-DSS v3.2.1.

NISTStack.template: normas del Instituto Nacional de Estándares y Tecnología (NIST), versión 5.0.0.

SCStack.template: reglas de Security Controls v2.0.0.

Funciones de los miembros

automa

security-response-member-roles.template: define las funciones de corrección necesarias en cada cuenta de miembro de AWS Security Hub.

Cuentas de miembros

automa

security-response-member.template: utilice esta plantilla después de configurar la solución principal para instalar los manuales de automatización y los permisos de AWS Systems Manager en cada una de las cuentas de los miembros de AWS Security Hub (incluida la cuenta de administrador). Esta plantilla le permite elegir qué manuales de normas de seguridad desea instalar.

`automated-security-response-member.template`Instala las siguientes plantillas en función de sus selecciones:

automated-security-response-remediation-runbooks.template: código de corrección común utilizado por uno o más de los estándares de seguridad.

AFSBPMemberStack.template: manuales de configuración, permisos y correcciones de AWS Foundational Security Best Practices v1.0.0.

CIS120 MemberStack .template: puntos de referencia de CIS Amazon Web Services Foundations, configuración de la versión 1.2.0, permisos y manuales de corrección.

CIS140 MemberStack .template: puntos de referencia de CIS Amazon Web Services Foundations, guías de configuración, permisos y correcciones de la versión 1.4.0.

CIS300 MemberStack .template: puntos de referencia de CIS Amazon Web Services Foundations, guías de configuración, permisos y correcciones de la versión 3.0.0.

PCI321MemberStack.template: manuales de configuración, permisos y correcciones de PCI-DSS v3.2.1.

NISTMemberStack.template: manuales de configuración, permisos y correcciones del Instituto Nacional de Estándares y Tecnología (NIST), versión 5.0.0.

SCMemberStack.template: manuales de configuración, permisos y correcciones del control de seguridad.

automated-security-response-member-cloudtrail.template: se utiliza en la función de registro de acciones para realizar un seguimiento, auditar y prestar servicio a la actividad.

Integración del sistema de tickets

Utilice una de las siguientes plantillas para integrarla con su sistema de venta de entradas.

JiraBlu

despliégalo si utilizas Jira como sistema de venta de entradas.

Service

despliégalo si lo utilizas ServiceNow como sistema de venta de entradas.

Si quieres integrar un sistema de venta de entradas externo diferente, puedes usar cualquiera de estas pilas como modelo para entender cómo implementar tu propia integración personalizada.

Despliegue automatizado: StackSets

> **Note**
>
> Recomendamos realizar la implementación con. StackSets Sin embargo, para las implementaciones con una sola cuenta o con fines de prueba o evaluación, considere la opción de implementación en pilas.

Antes de lanzar la solución, revise la arquitectura, los componentes de la solución, la seguridad y las consideraciones de diseño que se describen en esta guía. Siga las step-by-step instrucciones de esta sección para configurar e implementar la solución en sus AWS Organizations.

Tiempo de implementación: aproximadamente 30 minutos por cuenta, según StackSet los parámetros.

Requisitos previos

AWS Organizations le ayuda a gestionar y gobernar de forma centralizada su entorno y recursos de AWS con varias cuentas. StackSets funcionan mejor con AWS Organizations.

Si ya implementó la versión 1.3.x o una versión anterior de esta solución, debe desinstalar la solución existente. Para obtener más información, consulte Actualizar la solución.

Antes de implementar esta solución, revise la implementación de AWS Security Hub:

- Debe haber una cuenta de administrador de Security Hub delegada en su organización de AWS.
- Security Hub debe configurarse para agregar los hallazgos de todas las regiones. Para obtener más información, consulte Agregación de hallazgos en todas las regiones en la Guía del usuario de AWS Security Hub.
- Debe activar Security Hub para su organización en cada región en la que utilice AWS.

En este procedimiento se presupone que tiene varias cuentas que utilizan AWS Organizations y que ha delegado una cuenta de administrador de AWS Organizations y una cuenta de administrador de AWS Security Hub.

Descripción general de la implementación

> **Note**
>
> StackSets la implementación de esta solución utiliza una combinación de servicios gestionados y autogestionados. StackSets Los sistemas autogestionados se StackSets deben utilizar actualmente, ya que utilizan sistemas anidados StackSets, que aún no son compatibles con los servicios gestionados. StackSets

Impleméntelo StackSets desde una cuenta de administrador delegado en sus AWS Organizations.

Planificación

Utilice el siguiente formulario como ayuda con la StackSets implementación. Prepare los datos y, a continuación, copie y pegue los valores durante la implementación.

```
AWS Organizations admin account ID: _________________
```

```
Security Hub admin account ID: _________________
CloudTrail Logs Group: ____________________________
Member account IDs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
AWS Organizations OUs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
```

(Opcional) Paso 0: implementar la pila de integración de tickets

- Si tiene intención de utilizar la función de venta de entradas, implemente primero la pila de integración de venta de entradas en su cuenta de administrador de Security Hub.
- Copie el nombre de la función Lambda de esta pila y envíelo como entrada a la pila de administración (consulte el paso 1).

Paso 1: Inicie la pila de administración en la cuenta de administrador delegada de Security Hub

- Con una plantilla autogestionada StackSet, lance la CloudFormation plantilla de `automated-security-response-admin.template` AWS en su cuenta de administrador de AWS Security Hub en la misma región que su administrador de Security Hub. Esta plantilla utiliza pilas anidadas.
- Elija qué estándares de seguridad desea instalar. De forma predeterminada, solo se selecciona SC (recomendado).
- Elige un grupo de registros de Orchestrator existente para usarlo. Seleccione `Yes` si `SO0111-ASR- Orchestrator` ya existe en una instalación anterior.

Para obtener más información sobre la autogestión StackSets, consulte Otorgar permisos autogestionados en la Guía CloudFormation del usuario de AWS.

Paso 2: Instalar las funciones de corrección en cada cuenta de miembro de AWS Security Hub

Espere a que el paso 1 complete la implementación, ya que la plantilla del paso 2 hace referencia a las funciones de IAM creadas en el paso 1.

- Con un servicio gestionado StackSet, lance la CloudFormation plantilla de `automated-security-response-member-roles.template` AWS en una sola región de cada cuenta de AWS Organizations.
- Elija instalar esta plantilla automáticamente cuando una nueva cuenta se una a la organización.
- Introduzca el ID de cuenta de su cuenta de administrador de AWS Security Hub.

Paso 3: Lance la pila de miembros en cada cuenta y región de los miembros de AWS Security Hub

- De forma autogestionada StackSets, lance la CloudFormation plantilla de `automated-security-response-member.template` AWS en todas las regiones en las que tenga recursos de AWS en todas las cuentas de su organización de AWS administradas por el mismo administrador de Security Hub.

> **Note**
>
> Hasta que la administración de servicios dé StackSets soporte a las agrupaciones agrupadas, debe realizar este paso para todas las cuentas nuevas que se unan a la organización.

- Elija qué guías de normas de seguridad desea instalar.
- Proporcione el nombre de un grupo de CloudTrail registros (utilizado en algunas correcciones).
- Introduzca el ID de cuenta de su cuenta de administrador de AWS Security Hub.

(Opcional) Paso 0: lanzar una pila de integración del sistema de tickets

1. Si tiene intención de utilizar la función de venta de entradas, inicie primero la pila de integración correspondiente.
2. Elige los paquetes de integración proporcionados para Jira o ServiceNow úsalos como modelo para implementar tu propia integración personalizada.

   Para implementar el stack de Jira, sigue estos pasos:

   a. Introduce un nombre para tu pila.

   b. Proporciona el URI a tu instancia de Jira.

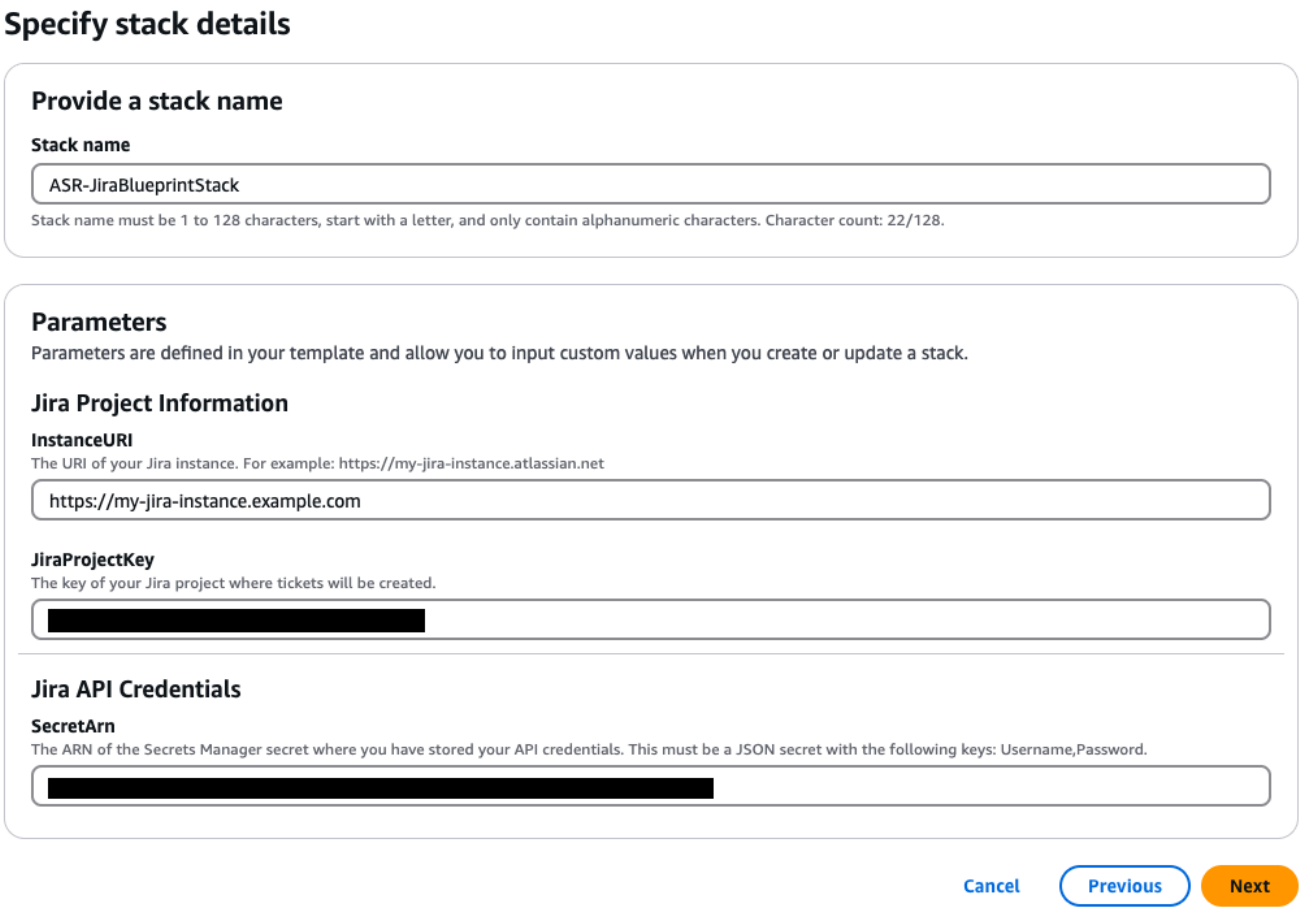
   c. Proporcione la clave del proyecto de Jira al que quiere enviar los tickets.

d. Crea un nuevo secreto clave-valor en Secrets Manager que contenga tu `Username` Jira y. `Password`

> **Note**
>
> Puede optar por utilizar una clave de API de Jira en lugar de su contraseña si proporciona su nombre de usuario `Username` y su clave de API como. `Password`

e. Agrega el ARN de este secreto como entrada a la pila.

Proporcione un nombre de pila, información del proyecto de Jira y credenciales de la API de Jira.



Para implementar la ServiceNow pila:

f. Introduce un nombre para tu pila.

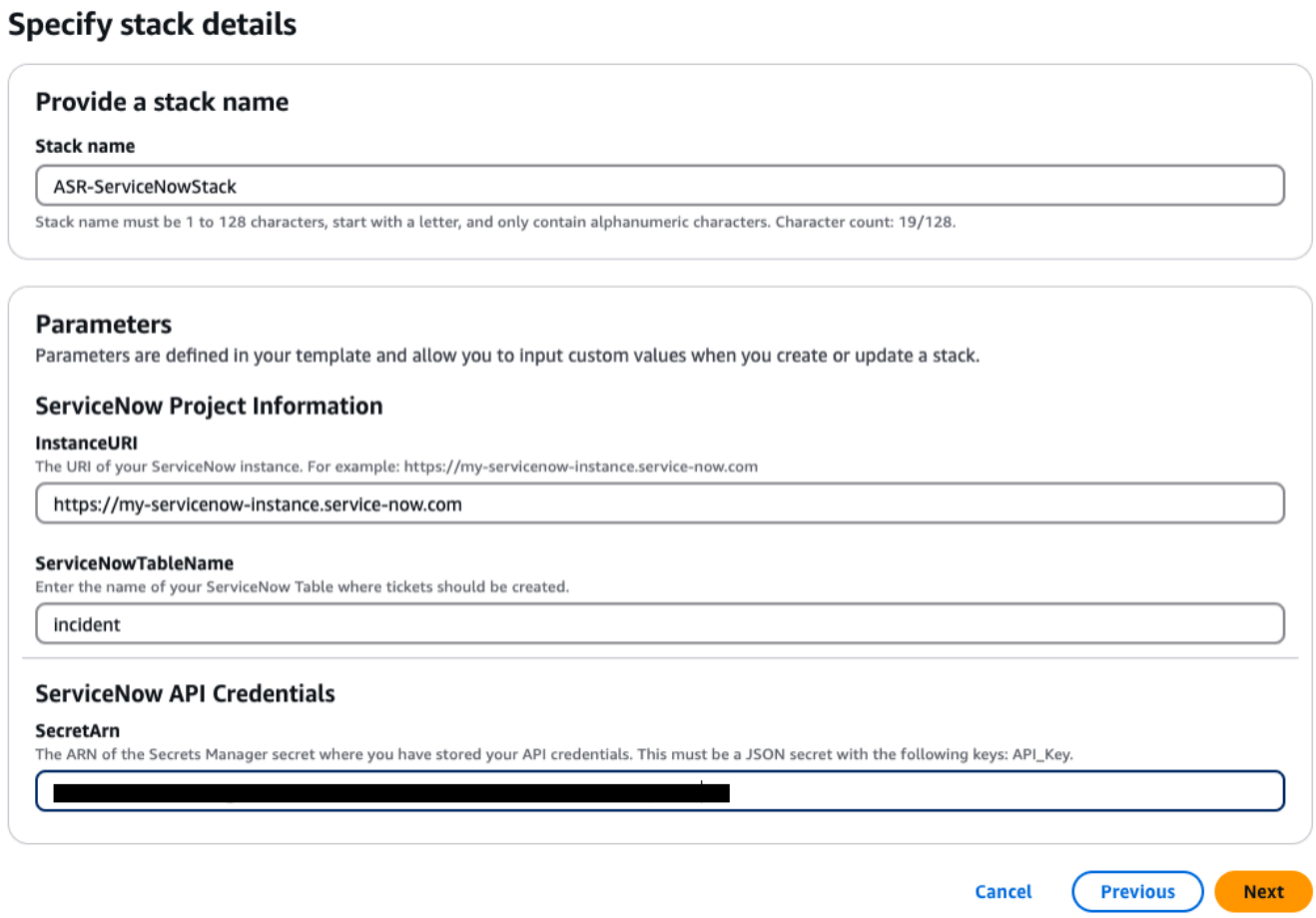
g. Proporcione el URI de la ServiceNow instancia.

h. Proporcione el nombre ServiceNow de la tabla.

i. Cree una clave de API ServiceNow con permiso para modificar la tabla en la que desea escribir.

j. Crea un secreto en Secrets Manager con la clave `API_Key` y proporciona el ARN secreto como entrada a la pila.

   Proporcione un nombre de pila, información ServiceNow del proyecto y credenciales de la ServiceNow API.

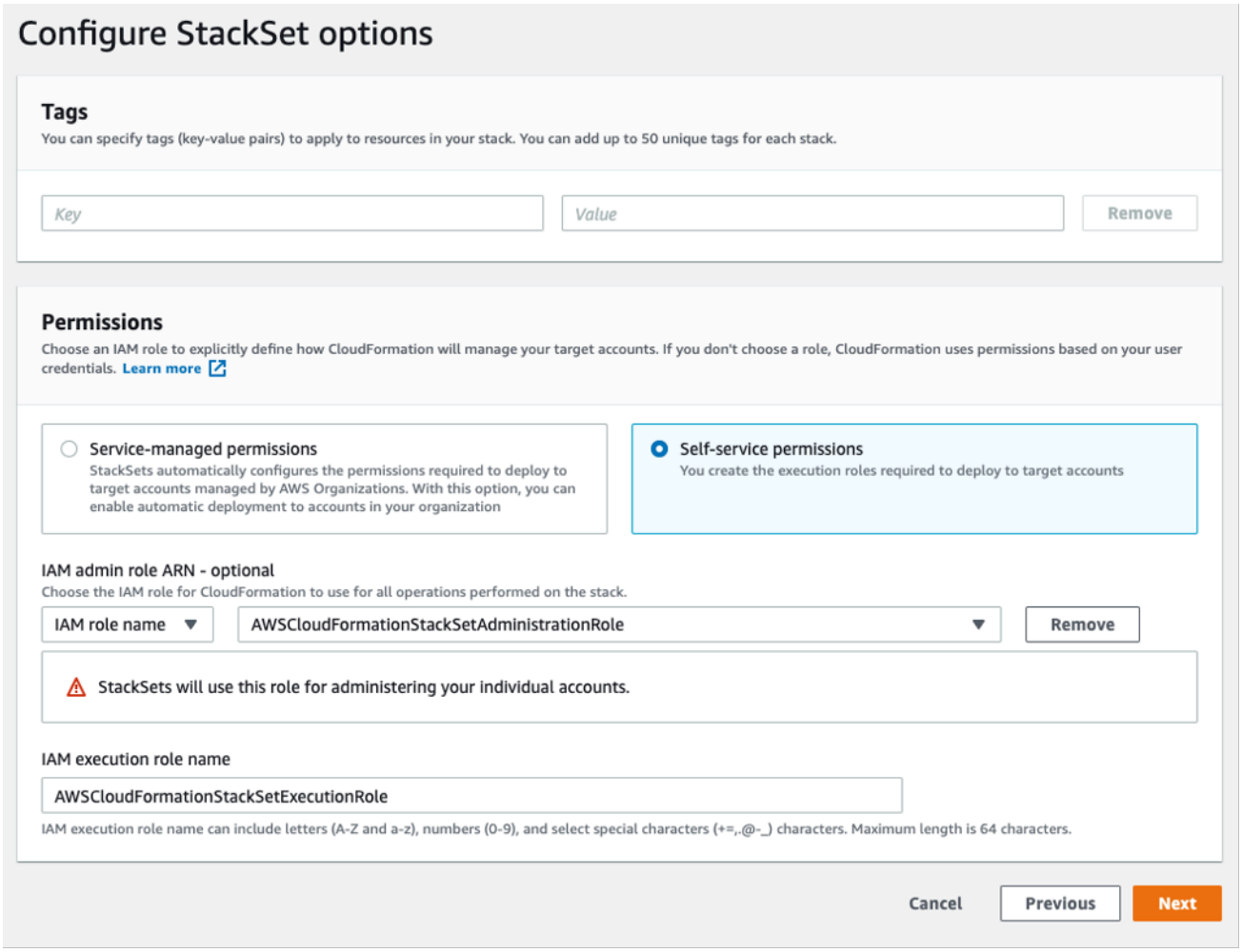


   Para crear una pila de integración personalizada: incluya una función Lambda que el orquestador de soluciones Step Functions pueda utilizar para cada corrección. La función Lambda debe tomar la entrada proporcionada por Step Functions, crear una carga útil de acuerdo con los requisitos del sistema de emisión de entradas y realizar una solicitud al sistema para que cree el billete.

Paso 1: Inicie la pila de administración en la cuenta de administrador delegada de Security Hub

1. Abre la pila de administración con tu cuenta de administrador de Security Hub. `automated-security-response-admin.template` Normalmente, uno por organización en una sola región. Como esta pila utiliza pilas anidadas, debes implementar esta plantilla como una plantilla autogestionada. StackSet

   Configure las opciones StackSet



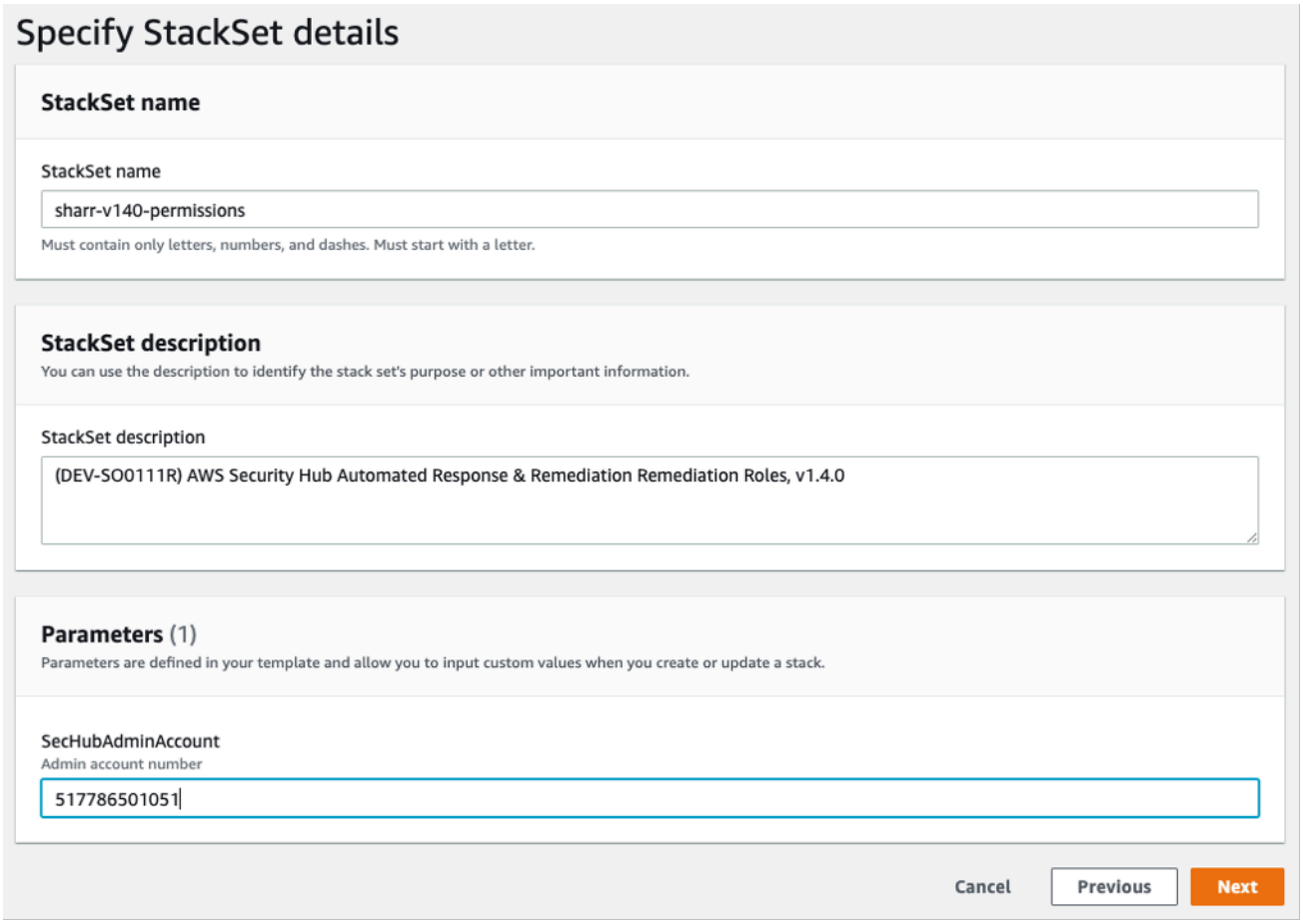
2. En el parámetro Números de cuenta, introduzca el ID de cuenta de la cuenta de administrador de AWS Security Hub.
3. En el parámetro Especificar regiones, selecciona solo la región en la que está activada la administración de Security Hub. Espere a que se complete este paso antes de continuar con el paso 2.

Paso 2: Instalar las funciones de corrección en cada cuenta de miembro de AWS Security Hub

Utilice un servicio gestionado StackSets para implementar la plantilla de roles de los miembros,. `automated-security-response-member-roles.template` StackSet Debe implementarse en una región por cuenta de miembro. Define las funciones globales que permiten las llamadas a la API entre cuentas desde la función escalonada de ASR Orchestrator.

1. Implemente en toda la organización (lo habitual) o en las unidades organizativas, según las políticas de su organización.
2. Active la implementación automática para que las nuevas cuentas de AWS Organizations reciban estos permisos.
3. En el parámetro Especificar regiones, seleccione una sola región. Las funciones de IAM son globales. Puede continuar con el paso 3 mientras se StackSet implementa.

   Especifique los detalles StackSet



Paso 3: Lance la pila de miembros en cada cuenta y región de los miembros de AWS Security Hub

Como la pila de miembros utiliza pilas anidadas, debe realizar la implementación de forma autogestionada. StackSet Esto no admite la implementación automática en cuentas nuevas de la organización de AWS.

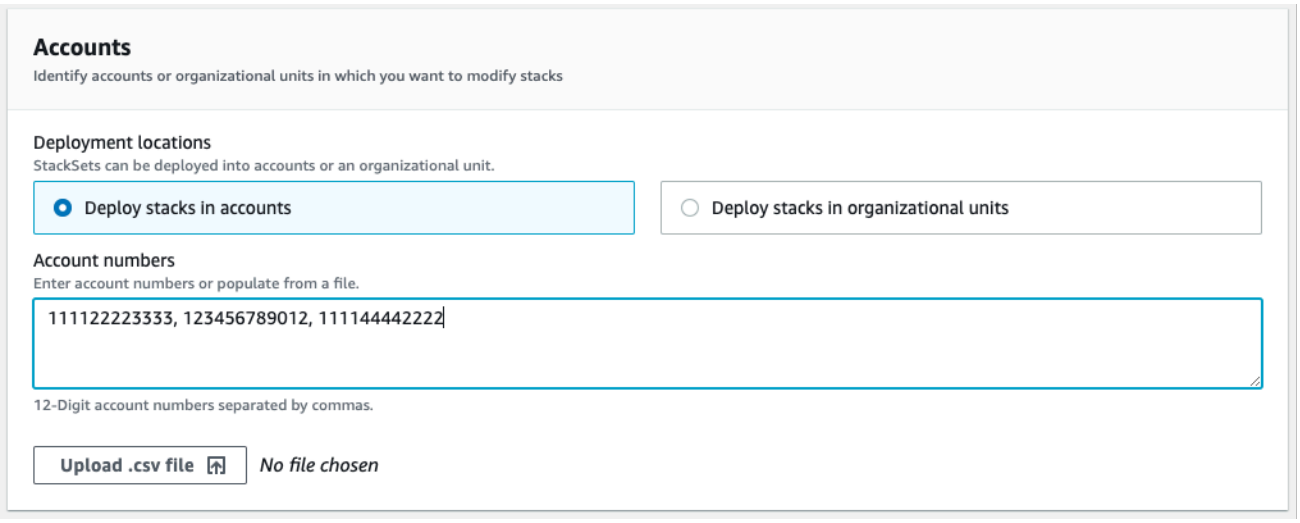
Parámetros

LogGroup Configuración: elija el grupo de registros que recibe CloudTrail los registros. Si no existe ninguno o si el grupo de registros es diferente para cada cuenta, elija un valor adecuado. Los administradores de cuentas deben actualizar el parámetro Systems Manager - Parameter Store/Solutions/SO0111/Metrics_ LogGroupName después de crear un grupo de CloudWatch registros para CloudTrail los registros. Esto es necesario para las correcciones que crean alarmas de métricas en las llamadas a la API.

Estándares: elija los estándares que desee cargar en la cuenta del miembro. Esto solo instala los manuales de ejecución de AWS Systems Manager, no habilita el estándar de seguridad.

SecHubAdminAccount: Introduzca el ID de cuenta de la cuenta de administrador de AWS Security Hub en la que instaló la plantilla de administración de la solución.

Cuentas



Ubicaciones de implementación: puede especificar una lista de números de cuenta o unidades organizativas.

Especifique las regiones: seleccione todas las regiones en las que desee corregir los hallazgos. Puede ajustar las opciones de despliegue según convenga en función del número de cuentas y regiones. La concurrencia regional puede ser paralela.

Despliegue automatizado: pilas

> **Note**
>
> Para los clientes con varias cuentas, recomendamos encarecidamente la implementación con StackSets.

Antes de lanzar la solución, revise la arquitectura, los componentes de la solución, la seguridad y las consideraciones de diseño que se describen en esta guía. Siga las step-by-step instrucciones de esta sección para configurar e implementar la solución en su cuenta.

Tiempo de implementación: aproximadamente 30 minutos

Requisitos previos

Antes de implementar esta solución, asegúrese de que AWS Security Hub esté en la misma región de AWS que sus cuentas principal y secundaria. Si ya implementó esta solución anteriormente, debe desinstalar la solución existente. Para obtener más información, consulte Actualizar la solución.

Descripción general de la implementación

Siga los siguientes pasos para implementar esta solución en AWS.

(Opcional) Paso 0: lanzar una pila de integración de sistemas de tickets

- Si tiene intención de utilizar la función de venta de entradas, implemente primero la pila de integración de venta de entradas en su cuenta de administrador de Security Hub.
- Copie el nombre de la función Lambda de esta pila y envíelo como entrada a la pila de administración (consulte el paso 1).

Paso 1: lanza la pila de administración

- Inicie la CloudFormation plantilla de `automated-security-response-admin.template` AWS en su cuenta de administrador de AWS Security Hub.

- Elija qué estándares de seguridad desea instalar.
- Elige un grupo de registros de Orchestrator existente para usarlo (`Yes`selecciónalo si `SO0111-ASR-Orchestrator` ya existe en una instalación anterior).

Paso 2: Instalar las funciones de corrección en cada cuenta de miembro de AWS Security Hub

- Lance la CloudFormation plantilla de `automated-security-response-member-roles.template` AWS en una región por cuenta de miembro.
- Introduzca el IG de 12 dígitos de la cuenta de administrador de AWS Security Hub.

Paso 3: Inicie la pila de miembros

- Especifique el nombre del grupo de CloudWatch registros que se utilizará con las correcciones de CIS 3.1-3.14. Debe ser el nombre de un grupo de CloudWatch registros que reciba registros. CloudTrail
- Elija si desea instalar las funciones de corrección. Instale estas funciones solo una vez por cuenta.
- Seleccione los libros de jugadas que desee instalar.
- Introduzca el ID de la cuenta de administrador de AWS Security Hub.

Paso 4: (opcional) Ajuste las soluciones disponibles

- Elimine cualquier corrección en función de la cuenta de cada miembro. Este paso es opcional.

(Opcional) Paso 0: lanzar una pila de integración de sistemas de tickets

1. Si tiene intención de utilizar la función de venta de entradas, inicie primero la pila de integración correspondiente.
2. Elige los paquetes de integración proporcionados para Jira o ServiceNow úsalos como modelo para implementar tu propia integración personalizada.

   Para implementar el stack de Jira, sigue estos pasos:

   a. Introduce un nombre para tu pila.

   b. Proporciona el URI a tu instancia de Jira.

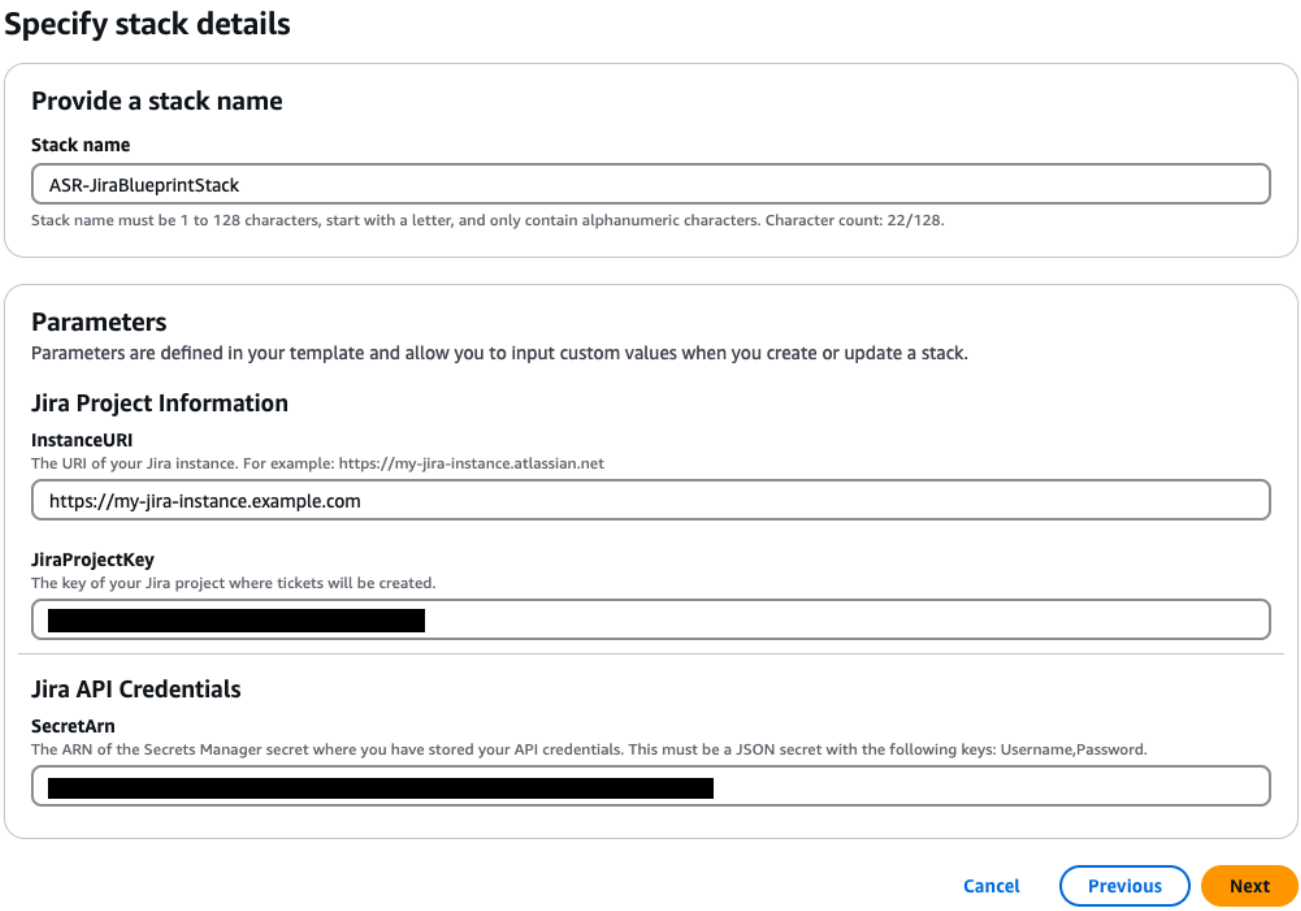
   c. Proporcione la clave del proyecto de Jira al que quiere enviar los tickets.

d. Crea un nuevo secreto clave-valor en Secrets Manager que contenga tu `Username` Jira y. `Password`

> **Note**
>
> Puede optar por utilizar una clave de API de Jira en lugar de su contraseña si proporciona su nombre de usuario `Username` y su clave de API como. `Password`

e. Agrega el ARN de este secreto como entrada a la pila.

«Proporcione un nombre de pila, información del proyecto de Jira y credenciales de la API de Jira.



Para implementar la ServiceNow pila:

f. Introduce un nombre para tu pila.

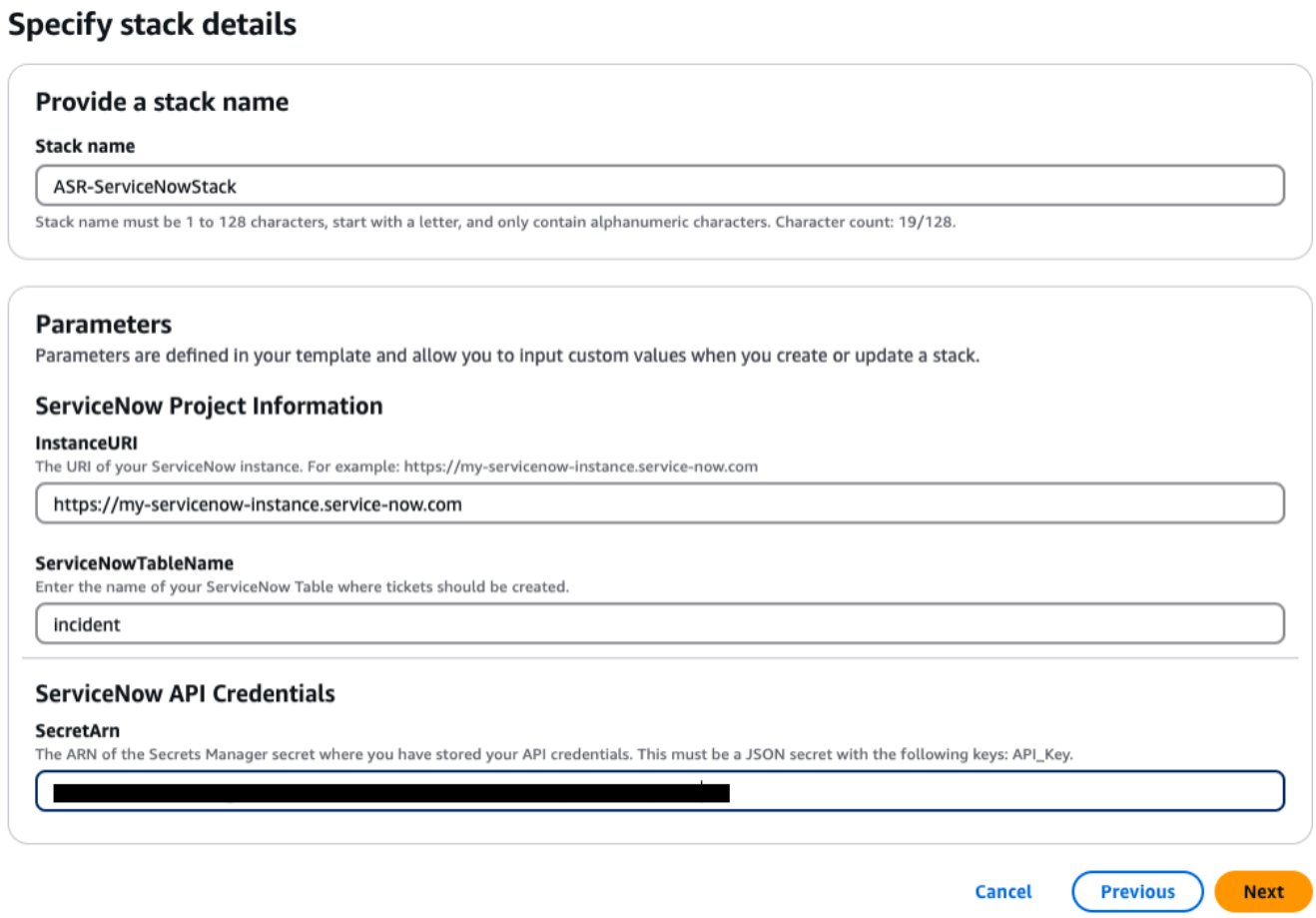
g. Proporcione el URI de la ServiceNow instancia.

h. Proporcione el nombre ServiceNow de la tabla.

i. Cree una clave de API ServiceNow con permiso para modificar la tabla en la que desea escribir.

j. Crea un secreto en Secrets Manager con la clave `API_Key` y proporciona el ARN secreto como entrada a la pila.

   Proporcione un nombre de pila, información ServiceNow del proyecto y credenciales de la ServiceNow API.



   Para crear una pila de integración personalizada: incluya una función Lambda que el orquestador de soluciones Step Functions pueda utilizar para cada corrección. La función Lambda debe tomar la entrada proporcionada por Step Functions, crear una carga útil de acuerdo con los requisitos del sistema de emisión de entradas y realizar una solicitud al sistema para que cree el billete.

Paso 1: Lanza la pila de administración

Important

Esta solución incluye una opción para enviar métricas operativas anonimizadas a AWS. Utilizamos estos datos para comprender mejor cómo utilizan los clientes esta solución, así como los servicios y productos relacionados. AWS es propietario de los datos recopilados a través de esta encuesta. La recopilación de datos está sujeta al Aviso de privacidad de AWS. Para excluirse de esta función, descargue la plantilla, modifique la sección de CloudFormation mapeo de AWS y, a continuación, utilice la CloudFormation consola de AWS para cargar la plantilla e implementar la solución. Para obtener más información, consulte la sección de recopilación de datos anonimizados de esta guía.

Esta CloudFormation plantilla automatizada de AWS implementa la solución Automated Security Response on AWS en la nube de AWS. Antes de lanzar la pila, debe habilitar Security Hub y cumplir los requisitos previos.

Note

Usted es responsable del coste de los servicios de AWS utilizados durante la ejecución de esta solución. Para obtener más información, visite la sección de costos de esta guía y consulte la página web de precios de cada servicio de AWS utilizado en esta solución.

1. Inicie sesión en la Consola de administración de AWS desde la cuenta en la que se encuentra configurado actualmente el AWS Security Hub y utilice el botón de abajo para lanzar la CloudFormation plantilla de `automated-security-response-admin.template` AWS.

   Launch solution

   También puede descargar la plantilla para usarla como punto de partida para su propia implementación.

2. La plantilla se lanza en la región Este de EE. UU. (Norte de Virginia) de forma predeterminada. Para lanzar esta solución en una región de AWS diferente, utilice el selector de regiones de la barra de navegación de la consola de administración de AWS.

> **Note**
>
> Esta solución utiliza AWS Systems Manager, que actualmente solo está disponible en regiones específicas de AWS. La solución funciona en todas las regiones que admiten este servicio. Para obtener la disponibilidad más reciente por región, consulte la lista de servicios regionales de AWS.

3. En la página Crear pila, compruebe que la URL de la plantilla correcta esté en el cuadro de texto URL de Amazon S3 y, a continuación, seleccione Siguiente.
4. En la página Especificar los detalles de la pila, especifique un nombre para la pila. Para obtener información sobre las limitaciones de nombres de caracteres, consulte los límites de IAM y STS en la Guía del usuario de AWS Identity and Access Management.
5. En la página de parámetros, seleccione Siguiente.

Parámetro	Predeterminado/a	Descripción
Cargue SC Admin Stack	`yes`	Especifique si desea instalar los componentes de administración para la corrección automática de los controles de SC.
Cargue la pila de administración de AFSBP	no	Especifique si desea instalar los componentes de administración para la corrección automática de los controles del FSBP.
Cargue 0 Admin Stack CIS12	no	Especifique si desea instalar los componentes de administración para la corrección automática de CIS12 0 controles.
Cargue CIS14 0 Admin Stack	no	Especifique si desea instalar los componentes de administr

Parámetro	Predeterminado/a	Descripción
		ación para la correcció n automática de CIS14 0 controles.
Cargue CIS3 00 Admin Stack	no	Especifique si desea instalar los componentes de administr ación para la correcció n automática de CIS3 00 controles.
Cargue PC1321 Admin Stack	no	Especifique si desea instalar los componentes de administr ación para la corrección automática de PC1321 los controles.
Cargue la pila de administr ación del NIST	no	Especifique si desea instalar los componentes de administr ación para la corrección automática de los controles del NIST.

Parámetro	Predeterminado/a	Descripción
Reutilice el grupo de registros de Orchestrator	no	Seleccione si desea reutilizar o no un grupo de `SO0111-ASR-Orchestrator` CloudWatch registros existente. Esto simplifica la reinstalación y las actualizaciones sin perder los datos de registro de una versión anterior. Reutilice la existente: `Orchestrator Log Group` elija `yes` si `Orchestrator Log Group` aún existe de una implementación anterior en esta cuenta; de lo contrario . no Si va a realizar una actualización de pila desde una versión anterior a la v2.3.0, elija no
Utilice métricas CloudWatch	`yes`	Especifique si desea habilitar CloudWatch las métricas para monitorear la solución. Esto creará un CloudWatch panel de control para ver las métricas.
Usa CloudWatch métricas y alarmas	`yes`	Especifique si desea activar CloudWatch las alarmas métricas para la solución. Esto creará alarmas para determinadas métricas recopiladas por la solución.

Parámetro	Predeterminado/a	Descripción
RemediationFailure AlarmThreshold	5	Especifique el umbral del porcentaje de errores de corrección por ID de control. Por ejemplo, si lo introduce5, recibirá una alarma si un ID de control no supera más del 5% de las correcciones en un día determinado. Este parámetro solo funciona si se crean alarmas (consulte el parámetro Use CloudWatch Metrics Alarms).
EnableEnhancedCloudWatchMetrics	no	Siyes, crea CloudWatch métricas adicionales para realizar un seguimiento de todos los controles de IDs forma individual en el CloudWatch panel de control y como CloudWatch alarmas. Consulte la sección de costos para comprender el costo adicional en el que incurre.
TicketGenFunctionName	(Entrada opcional)	Opcional. Déjelo en blanco si no quiere integrar un sistema de venta de entradas. De lo contrario, proporcione el nombre de la función Lambda del resultado de la pila del paso 0, por ejemplo:. `SO0111-ASR-ServiceNow-TicketGenerator`

Parámetro	Predeterminado/a	Descripción
TargetAccountIDs	`ALL`	Una lista de cuentas de AWS IDs para controlar el alcance de la corrección automática. Utilice «TODAS» para dirigirse a todas las cuentas de la organización. O bien, proporcione una lista separada por comas de la cuenta de AWS de 12 dígitos. IDs Ejemplo: «12345678 9012,098765432109"
TargetAccountIDsStrategy (Estrategia)	`INCLUDE`	Define la forma en que la solución aplica las correccio nes automatizadas en función de la lista. TargetAccount IDs INCLUYE: ejecute correccio nes automatizadas solo para las cuentas de la lista. EXCLUIR: ejecute correccio nes automáticas para todas las cuentas, excepto para las que aparecen en la lista.

> **Note**
>
> Debe habilitar manualmente las correcciones automáticas en la cuenta de administrador después de implementar o actualizar las pilas de CloudFormation soluciones.

1. En la página Configurar opciones de pila, elija Siguiente.

2. En la página Revisar, revise y confirme la configuración. Marque la casilla para confirmar que la plantilla creará recursos de AWS Identity and Access Management (IAM).
3. Elija Create stack (Crear pila) para implementar la pila.

Puede ver el estado de la pila en la CloudFormation consola de AWS en la columna Estado. Debería recibir el estado CREATE_COMPLETE en aproximadamente 15 minutos.

Paso 2: Instalar las funciones de corrección en cada cuenta de miembro de AWS Security Hub

Solo se `automated-security-response-member-roles.template` StackSet deben implementar en una región por cuenta de miembro. Define las funciones globales que permiten las llamadas a la API entre cuentas desde la función escalonada de ASR Orchestrator.

1. Inicie sesión en la Consola de administración de AWS para cada cuenta de miembro de AWS Security Hub (incluida la cuenta de administrador, que también es miembro). Seleccione el botón para lanzar la CloudFormation plantilla de `automated-security-response-member-roles.template` AWS. También puede descargar la plantilla para usarla como punto de partida para su propia implementación.

2. La plantilla se lanza en la región Este de EE. UU. (Norte de Virginia) de forma predeterminada. Para lanzar esta solución en una región de AWS diferente, utilice el selector de regiones de la barra de navegación de la consola de administración de AWS.
3. En la página Crear pila, compruebe que la URL de la plantilla correcta esté en el cuadro de texto URL de Amazon S3 y, a continuación, seleccione Siguiente.
4. En la página Especificar los detalles de la pila, especifique un nombre para la pila. Para obtener información sobre las limitaciones de nombres de caracteres, consulte los límites de IAM y STS en la Guía del usuario de AWS Identity and Access Management.
5. En la página de parámetros, especifique los siguientes parámetros y seleccione Siguiente.

Parámetro	Predeterminado/a	Descripción
Namespace	*<Requires input>*	Introduzca una cadena de hasta 9 caracteres alfanumér

Parámetro	Predeterminado/a	Descripción
		icos en minúscula. Espacio de nombres único que se añadirá como sufijo a los nombres de las funciones de IAM de corrección. Se debe usar el mismo espacio de nombres en los roles de los miembros y en las pilas de miembros. Esta cadena debe ser única para cada implementación de soluciones, pero no es necesario cambiarla durante las actualizaciones de la pila. No es necesario que el valor del espacio de nombres sea único por cuenta de miembro.
Administrador de cuentas de Sec Hub	*<Requires input>*	Introduzca el ID de cuenta de 12 dígitos de la cuenta de administrador de AWS Security Hub. Este valor otorga permisos al rol de solución de la cuenta de administrador.

6. En la página Configurar opciones de pila, elija Siguiente.
7. En la página Revisar, revise y confirme la configuración. Marque la casilla para confirmar que la plantilla creará recursos de AWS Identity and Access Management (IAM).
8. Elija Create stack (Crear pila) para implementar la pila.

   Puede ver el estado de la pila en la CloudFormation consola de AWS en la columna Estado. Debería recibir el estado CREATE_COMPLETE en aproximadamente 5 minutos. Puede continuar con el siguiente paso mientras se carga la pila.

Paso 3: lanza la pila de miembros

> **Important**
>
> Esta solución incluye una opción para enviar métricas operativas anonimizadas a AWS. Utilizamos estos datos para comprender mejor cómo utilizan los clientes esta solución, así como los servicios y productos relacionados. AWS es propietario de los datos recopilados a través de esta encuesta. La recopilación de datos está sujeta a la Política de privacidad de AWS.
>
> Para excluirse de esta función, descargue la plantilla, modifique la sección de CloudFormation mapeo de AWS y, a continuación, utilice la CloudFormation consola de AWS para cargar la plantilla e implementar la solución. Para obtener más información, consulte la sección Recopilación de métricas operativas de esta guía.

La `automated-security-response-member` pila debe estar instalada en la cuenta de cada miembro de Security Hub. Esta pila define los manuales para la corrección automática. El administrador de cada cuenta de miembro puede controlar qué soluciones están disponibles a través de esta pila.

1. Inicie sesión en la Consola de administración de AWS para cada cuenta de miembro de AWS Security Hub (incluida la cuenta de administrador, que también es miembro). Seleccione el botón para lanzar la CloudFormation plantilla de `automated-security-response-member.template` AWS.

   Launch solution

También puede descargar la plantilla como punto de partida para su propia implementación. La plantilla se lanza en la región Este de EE. UU. (Norte de Virginia) de forma predeterminada. Para lanzar esta solución en una región de AWS diferente, utilice el selector de regiones de la barra de navegación de la consola de administración de AWS.

+

> **Note**
>
> Esta solución utiliza AWS Systems Manager, que actualmente está disponible en la mayoría de las regiones de AWS. La solución funciona en todas las regiones que admiten estos servicios. Para obtener la disponibilidad más reciente por región, consulte la lista de servicios regionales de AWS.

1. En la página Crear pila, compruebe que la URL de la plantilla correcta esté en el cuadro de texto URL de Amazon S3 y, a continuación, seleccione Siguiente.
2. En la página Especificar los detalles de la pila, especifique un nombre para la pila. Para obtener información sobre las limitaciones de nombres de caracteres, consulte los límites de IAM y STS en la Guía del usuario de AWS Identity and Access Management.
3. En la página de parámetros, especifique los siguientes parámetros y seleccione Siguiente.

Parámetro	Predeterminado/a	Descripción
Indique el nombre del LogGroup que se va a utilizar para crear filtros métricos y alarmas	*<Requires input>*	Especifique el nombre del grupo de CloudWatch CloudTrail registros donde se registran las llamadas a la API. Se utiliza para las correcciones de CIS 3.1-3.14.
Cargue la pila de miembros de SC	`yes`	Especifique si desea instalar los componentes miembros para la reparación automática de los controles del SC.
Cargue la pila de miembros de AFSBP	no	Especifique si desea instalar los componentes miembros para la corrección automática de los controles del FSBP.
Cargue una pila de 0 miembros CIS12	no	Especifique si desea instalar los componentes miembros

Parámetro	Predeterminado/a	Descripción
		para la corrección automática de CIS12 0 controles.
Cargue una CIS14 pila de 0 miembros	no	Especifique si desea instalar los componentes miembros para la corrección automática de CIS14 0 controles.
Cargue una CIS3 pila de 00 miembros	no	Especifique si desea instalar los componentes miembros para la corrección automática de CIS3 00 controles.
Cargue la pila PC1321 de miembros	no	Especifique si desea instalar los componentes miembros para la corrección automática de PC1321 los controles.
Cargue la pila de miembros del NIST	no	Especifique si desea instalar los componentes miembros para la corrección automática de los controles del NIST.
Cree un bucket de S3 para el registro de auditoría de Redshift	no	Seleccione `yes` si se debe crear el depósito de S3 para la corrección de FSBP 4.4. RedShift Para obtener más información sobre el bucket de S3 y la correcció n, consulte la corrección de Redshift.4 en la Guía del usuario de AWS Security Hub.

Parámetro	Predeterminado/a	Descripción
Cuenta de administrador de Sec Hub	*<Requires input>*	Introduzca el ID de cuenta de 12 dígitos de la cuenta de administrador de AWS Security Hub.
Namespace	*<Requires input>*	Introduzca una cadena de hasta 9 caracteres alfanuméricos en minúscula. Esta cadena pasa a formar parte de los nombres de las funciones de IAM y del bucket de Action Log S3. Utilice el mismo valor para el despliegue de la pila de miembros y para el despliegue de la pila de roles de miembros. La cadena debe ser única para cada implementación de soluciones, pero no es necesario cambiarla durante las actualizaciones de la pila.

Parámetro	Predeterminado/a	Descripción
EnableCloudTrailForASRActionLog (Registro)	no	Seleccione esta opción `yes` si desea supervisar los eventos de administración que lleva a cabo la solución en el CloudWatch panel de control. La solución crea un CloudTrail registro en cada cuenta de miembro que seleccione`yes`. Debe implementar la solución en una organización de AWS para habilitar esta función. Consulte la sección de costos para comprender el costo adicional que esto implica.

4. En la página Configurar opciones de pila, elija Siguiente.
5. En la página Revisar, revise y confirme la configuración. Marque la casilla para confirmar que la plantilla creará recursos de AWS Identity and Access Management (IAM).
6. Elija Create stack (Crear pila) para implementar la pila.

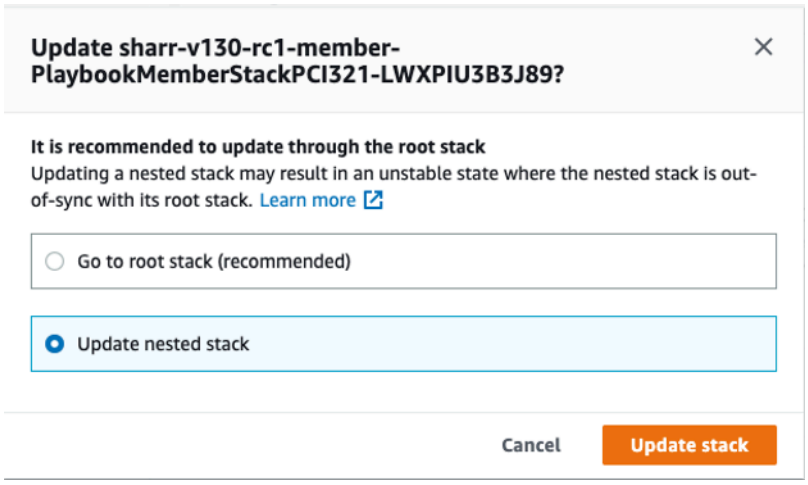
Puede ver el estado de la pila en la CloudFormation consola de AWS en la columna Estado. Debería recibir el estado CREATE_COMPLETE en aproximadamente 15 minutos.

Paso 4: (opcional) Ajustar las soluciones disponibles

Si quieres eliminar soluciones específicas de la cuenta de un miembro, puedes hacerlo actualizando la pila anidada según el estándar de seguridad. Para simplificar, las opciones de pila anidada no se propagan a la pila raíz.

1. Inicie sesión en la CloudFormation consola de AWS y seleccione la pila anidada.
2. Elija Actualizar.
3. Seleccione Actualizar pila anidada y elija Actualizar pila.

   Actualiza la pila anidada



4. Seleccione Usar la plantilla actual y elija Siguiente.
5. Ajuste las soluciones disponibles. Cambie los valores de los controles deseados a `Available` y los no deseados a. `Not available`

> **Note**
>
> Al desactivar una corrección, se elimina el manual de corrección de soluciones para el estándar de seguridad y el control.

6. En la página Configurar opciones de pila, elija Siguiente.
7. En la página Revisar, revise y confirme la configuración. Marque la casilla para confirmar que la plantilla creará recursos de AWS Identity and Access Management (IAM).
8. Seleccione Actualizar pila.

Puede ver el estado de la pila en la CloudFormation consola de AWS en la columna Estado. Debería recibir el estado CREATE_COMPLETE en aproximadamente 15 minutos.

Despliegue de la Torre de Control (CT)

La guía de personalizaciones para la Torre de Control de AWS (cFCT) está destinada a administradores, DevOps profesionales, proveedores de software independientes, arquitectos de infraestructuras de TI e integradores de sistemas que desean personalizar y ampliar sus entornos de torres de control de AWS para su empresa y sus clientes. Proporciona información sobre cómo personalizar y ampliar el entorno de AWS Control Tower con el paquete de personalización CfCT.

Tiempo de implementación: aproximadamente 30 minutos

Requisitos previos

Antes de implementar esta solución, asegúrese de que está destinada a los administradores de la Torre de Control de AWS.

Cuando esté listo para configurar su landing zone con la consola de AWS Control Tower o APIs siga estos pasos:

Para empezar a usar AWS Control Tower, consulte: Introducción a AWS Control Tower

Para obtener información sobre cómo personalizar tu zona de aterrizaje, consulta: Personalización de tu zona de aterrizaje

Para lanzar y desplegar tu zona de aterrizaje, consulta: Guía de despliegue de landing zone

Descripción general de la implementación

Siga los siguientes pasos para implementar esta solución en AWS.

Paso 1: Cree e implemente un bucket de S3

> **Note**
>
> Configuración del bucket de S3: solo para administradores. Este paso de configuración se realiza una sola vez y los usuarios finales no deben repetirlo. Los buckets de S3 almacenan el paquete de implementación, que incluye la CloudFormation plantilla de AWS y el código Lambda necesarios para la ejecución de ASR. Estos recursos se implementan mediante CfCt o. StackSet

1. Configure el bucket de S3

Configure el depósito de S3 que se utilizará para almacenar y servir los paquetes de despliegue.

2. Configuración del entorno de

Prepare las variables de entorno, las credenciales y las herramientas necesarias para el proceso de creación e implementación.

3. Configure las políticas de bucket de S3

Defina y aplique las políticas de bucket adecuadas para controlar el acceso y los permisos.

4. Prepare la compilación

Compila, empaquete o prepara de otro modo la aplicación o los activos para su implementación.

5. Implemente paquetes en S3

Cargue los artefactos de construcción preparados en el depósito de S3 designado.

Paso 2: Apila la implementación en la Torre de Control de AWS

1. Cree un manifiesto de compilación para los componentes de ASR

Defina un manifiesto de compilación que enumere todos los componentes de ASR, sus versiones, dependencias e instrucciones de compilación.

2. Actualice el CodePipeline

Modifique la CodePipeline configuración de AWS para incluir los nuevos pasos de compilación, artefactos o etapas necesarios para implementar los componentes de ASR.

Paso 1: Cree e implemente en un bucket de S3

Las soluciones de AWS utilizan dos grupos: un grupo para el acceso global a las plantillas, al que se accede a través de HTTPS, y grupos regionales para el acceso a los activos de la región, como el código Lambda.

1. Configure el bucket de S3

Elija un nombre de bucket único, por ejemplo, asr-staging. Defina dos variables de entorno en su terminal: una debe ser el nombre del bucket base con -reference como sufijo y la otra con la región de despliegue prevista como sufijo:

```
export BASE_BUCKET_NAME=asr-staging-$(date +%s)
export TEMPLATE_BUCKET_NAME=$BASE_BUCKET_NAME-reference
export REGION=us-east-1
export ASSET_BUCKET_NAME=$BASE_BUCKET_NAME-$REGION
```

2. Configuración del entorno

En su cuenta de AWS, cree dos buckets con estos nombres, por ejemplo, asr-staging-reference y asr-staging-us-east -1. (El grupo de referencia contendrá las CloudFormation plantillas, el grupo regional contendrá todos los demás activos, como el paquete de código lambda). Sus depósitos deben estar cifrados y no permitir el acceso público

```
aws s3 mb s3://$TEMPLATE_BUCKET_NAME/
aws s3 mb s3://$ASSET_BUCKET_NAME/
```

> **Note**
>
> Al crear tus depósitos, asegúrate de que no sean de acceso público. Usa nombres de cubos aleatorios. Deshabilita el acceso público. Utilice el cifrado KMS. Y compruebe la propiedad del bucket antes de subirlo.

3. Configuración de la política de cubos de S3

Actualice la política de bucket de S3 $TEMPLATE_BUCKET_NAME para incluir los permisos para el ID de la cuenta de ejecución. PutObject Asigne este permiso a una función de IAM dentro de la cuenta de ejecución que esté autorizada a escribir en el bucket. Esta configuración le permite evitar crear el depósito en la cuenta de administración.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::<template bucket name>/*",
                "arn:aws:s3:::<template bucket name>"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "<org id>"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::<template bucket name>/*",
                "arn:aws:s3:::<template bucket name>"
```

```
            ],
            "Condition": {
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::<execute_account_id>:role/
<iam_role_name>"
                }
            }
        }
    ]
}
```

Modifique la política de depósitos de S3 de los activos para incluir los permisos. Asigne este permiso a una función de IAM dentro de la cuenta de ejecución que esté autorizada a escribir en el bucket. Repita esta configuración para cada grupo de activos regional (por ejemplo, asr-staging-us-east -1, asr-staging-eu-west -1, etc.), lo que permitirá realizar despliegues en varias regiones sin necesidad de crear los grupos en la cuenta de administración.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::<asset bucket name>-<region>/*",
                "arn:aws:s3:::<asset bucket name>-<region>"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "<org id>"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
            "arn:aws:s3:::<asset bucket name>-<region>/*",
                "arn:aws:s3:::<asset bucket name>-<region>"
            ],
            "Condition": {
```

```
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::<execute_account_id>:role/
<iam_role_name>"
                }
            }
        }
    ]
}
```

4. Preparación de la compilación

- Requisitos previos:
  - Versión 2 de AWS CLI
  - Python 3.11+ con pip
  - AWS CDK 2.171.1 O SUPERIOR
  - Node.js 20+ con npm
  - Poetry v2 con complemento para exportar
- Clon de Git https://github.com/aws-solutions/automated-security-response-on-aws.git

Primero asegúrate de haber ejecutado npm install en la carpeta de origen.

A continuación, desde la carpeta de despliegue del repositorio clonado, ejecuta build-s3-dist.sh y pasa el nombre raíz del depósito (por ejemplo, mybucket) y la versión que estás creando (por ejemplo, la versión 1.0.0). Recomendamos usar una versión de semver basada en la versión descargada (p. ej. GitHub GitHub: v1.0.0, tu compilación: v1.0.0.mybuild)

```
chmod +x build-s3-dist.sh
export SOLUTION_NAME=automated-security-response-on-aws
export SOLUTION_VERSION=v1.0.0.mybuild
./build-s3-dist.sh -b $BASE_BUCKET_NAME -v $SOLUTION_VERSION
```

5. Implemente paquetes en S3

```
cd deployment
aws s3 cp global-s3-assets/  s3://$TEMPLATE_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive --acl bucket-owner-full-control
aws s3 cp regional-s3-assets/  s3://$ASSET_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive --acl bucket-owner-full-control
```

Paso 2: Apila la implementación en la Torre de Control de AWS

1. Cree un manifiesto para los componentes de ASR

Después de implementar los artefactos de ASR en los buckets de S3, actualice el manifiesto de la canalización de la Torre de Control para que haga referencia a la nueva versión y, a continuación, active la ejecución de la canalización, consulte: implementación de la torre de control

> **Important**
>
> Para garantizar la implementación correcta de la solución ASR, consulte la documentación oficial de AWS para obtener información detallada sobre la descripción general de las CloudFormation plantillas y los parámetros. Los enlaces de información figuran a continuación: Guía general de los parámetros de las CloudFormation plantillas

El manifiesto de los componentes de ASR tiene el siguiente aspecto:

```
region: us-east-1 #<HOME_REGION_NAME>
version: 2021-03-15

# Control Tower Custom CloudFormation Resources
resources:
  - name: <ADMIN STACK NAME>
    resource_file: s3://<ADMIN TEMPLATE BUCKET path>
    parameters:
      - parameter_key: UseCloudWatchMetricsAlarms
        parameter_value: "yes"
      - parameter_key: TicketGenFunctionName
        parameter_value: ""
      - parameter_key: LoadSCAdminStack
        parameter_value: "yes"
      - parameter_key: LoadCIS120AdminStack
        parameter_value: "no"
      - parameter_key: TargetAccountIDsStrategy
        parameter_value: "INCLUDE"
      - parameter_key: LoadCIS300AdminStack
        parameter_value: "no"
      - parameter_key: UseCloudWatchMetrics
        parameter_value: "yes"
      - parameter_key: LoadNIST80053AdminStack
        parameter_value: "no"
```

```
      - parameter_key: LoadCIS140AdminStack
        parameter_value: "no"
      - parameter_key: ReuseOrchestratorLogGroup
        parameter_value: "yes"
      - parameter_key: LoadPCI321AdminStack
        parameter_value: "no"
      - parameter_key: RemediationFailureAlarmThreshold
        parameter_value: "5"
      - parameter_key: LoadAFSBPAdminStack
        parameter_value: "no"
      - parameter_key: TargetAccountIDs
        parameter_value: "ALL"
      - parameter_key: EnableEnhancedCloudWatchMetrics
        parameter_value: "no"
    deploy_method: stack_set
    deployment_targets:
     accounts: # :type: list
        - <ACCOUNT_NAME> # and/or
        - <ACCOUNT_NUMBER>
    regions:
      - <REGION_NAME>

  - name:  <ROLE MEMBER STACK NAME>
    resource_file: s3://<ROLE MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: Namespace
        parameter_value: <NAMESPACE>
    deploy_method: stack_set
    deployment_targets:
      organizational_units:
        - <ORG UNIT>

  - name:  <MEMBER STACK NAME>
    resource_file: s3://<MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: LoadCIS120MemberStack
        parameter_value: "no"
      - parameter_key: LoadNIST80053MemberStack
        parameter_value: "no"
      - parameter_key: Namespace
```

```
      parameter_value: <NAMESPACE>
    - parameter_key: CreateS3BucketForRedshiftAuditLogging
      parameter_value: "no"
    - parameter_key: LoadAFSBPMemberStack
      parameter_value: "no"
    - parameter_key: LoadSCMemberStack
      parameter_value: "yes"
    - parameter_key: LoadPCI321MemberStack
      parameter_value: "no"
    - parameter_key: LoadCIS140MemberStack
      parameter_value: "no"
    - parameter_key: EnableCloudTrailForASRActionLog
      parameter_value: "no"
    - parameter_key: LogGroupName
      parameter_value: <LOG_GROUP_NAME>
    - parameter_key: LoadCIS300MemberStack
      parameter_value: "no"
  deploy_method: stack_set
  deployment_targets:
   accounts: # :type: list
      - <ACCOUNT_NAME> # and/or
      - <ACCOUNT_NUMBER>
  organizational_units:
    - <ORG UNIT>
  regions: # :type: list
    - <REGION_NAME>
```

2. Actualización de la canalización de códigos

Agregue un archivo de manifiesto a un custom-control-tower-configuration archivo.zip y ejecute un CodePipeline, consulte: descripción general de la canalización de códigos

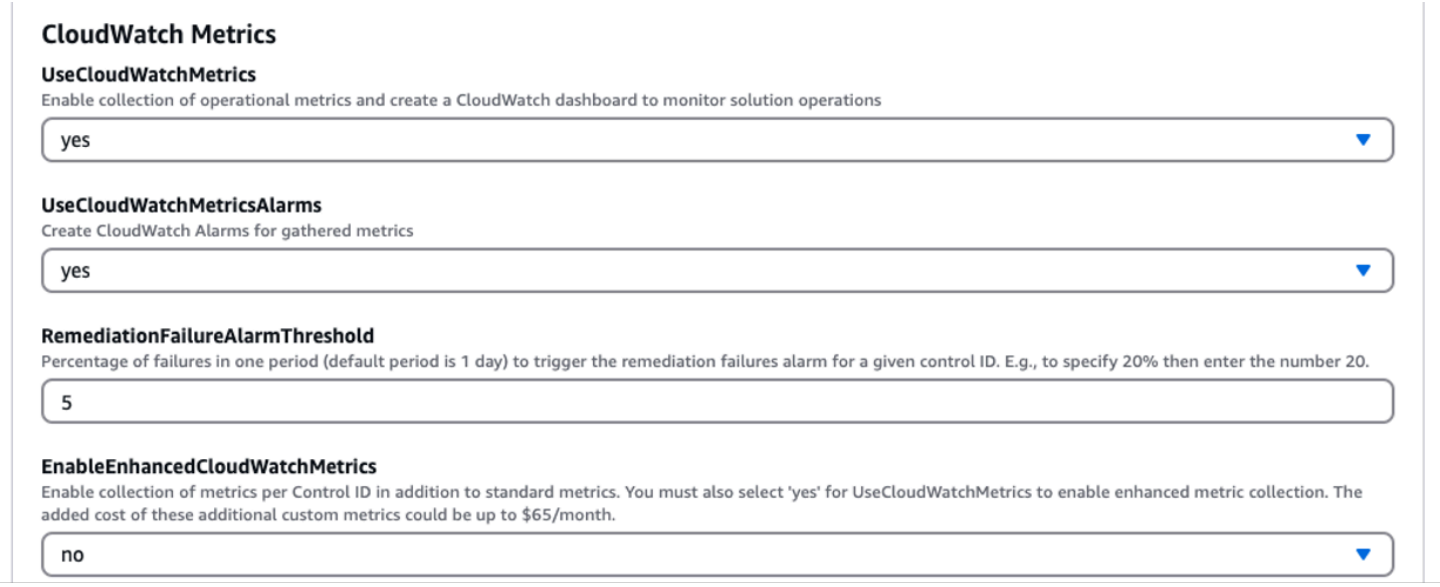
Supervisa las operaciones de la solución con un CloudWatch panel de Amazon

Esta solución incluye métricas y alarmas personalizadas que se muestran en un CloudWatch panel de Amazon.

El CloudWatch panel de control y las alarmas supervisan las operaciones de la solución y avisan cuando existe un posible problema.

Habilita CloudWatch las métricas, las alarmas y el panel

Hay cuatro parámetros CloudFormation de plantilla para la CloudWatch funcionalidad.



1. UseCloudWatchMetrics- Al configurarlo, se `yes` habilita la recopilación de métricas operativas y se crea un CloudWatch panel para ver estas métricas.
2. UseCloudWatchAlarms- Si lo configuras, `yes` se activan las alarmas predeterminadas de la solución.
3. RemediationFailureAlarmThreshold- El porcentaje de soluciones fallidas en un período en el que se emitió una alarma.
4. EnableEnhancedCloudWatchMetrics- Defina este parámetro `yes` para recopilar métricas individuales por ID de control. De forma predeterminada, este parámetro está establecido enno, de modo que solo se recopilan las métricas sobre el número total de correcciones en todos IDs los controles. Las métricas y alarmas individuales por ID de control conllevan un coste adicional.

Uso del panel de CloudWatch control

Para ver el panel:

1. Ve a Amazon CloudWatch y, a continuación, a Dashboards.
2. Selecciona el panel denominado «ASR-Remediation-Metrics-Dashboard».

El panel contiene las siguientes secciones: CloudWatch

1. Total de soluciones exitosas: le proporciona información sobre el número de hallazgos de Security Hub que la solución ha solucionado satisfactoriamente.
2. Errores de corrección: muestra el número de soluciones que han fallado, tanto en total como en porcentaje, y la causa del error. Un número elevado de errores puede indicar la existencia de un problema técnico con la solución que tal vez deba investigarse con más detalle.
3. Corrección correcta o fallida por ID de control: si activó las métricas mejoradas en el momento de la implementación, en esta sección se enumeran los resultados de las correcciones por ID de control. Si la sección de errores de corrección muestra una tasa de errores alta en general, en esta sección se muestra si los errores se distribuyen entre muchos controles o si solo algunos de IDs ellos están fallando. IDs
4. Runbook Assume Role Failles: muestra el número de errores que se produjeron debido a los intentos de corrección en cuentas que no tenían instalada la función de miembro de la solución. Los errores repetidos debidos a intentos de corrección automatizados debidos a la falta de funciones generan costes innecesarios. Mitigue esta situación instalando la pila de roles de miembro en las cuentas correspondientes, deshabilitando todas EventBridge las reglas creadas por la solución o desasociando la cuenta en Security Hub.
5. Acciones de administración de Cloud Trail de ASR: enumera las acciones de administración de la solución en todas las cuentas de los miembros en las que se habilitaron los registros de acciones con el parámetro EnableCloudTrailForASRActionLog en el momento de la implementación. Si observa cambios inesperados en los recursos en cualquiera de sus cuentas de AWS, este widget puede ayudarle a comprender si la solución modificó los recursos.

El CloudWatch panel también incluye alarmas predefinidas que alertan sobre errores operativos comunes.

1. State Machine ejecuta más de 1000 en un período de 24 horas.

   a. Un gran aumento en las ejecuciones de medidas correctivas podría indicar que una regla de eventos se está iniciando con más frecuencia de la prevista.

   b. El umbral se puede cambiar mediante el CloudFormation parámetro.

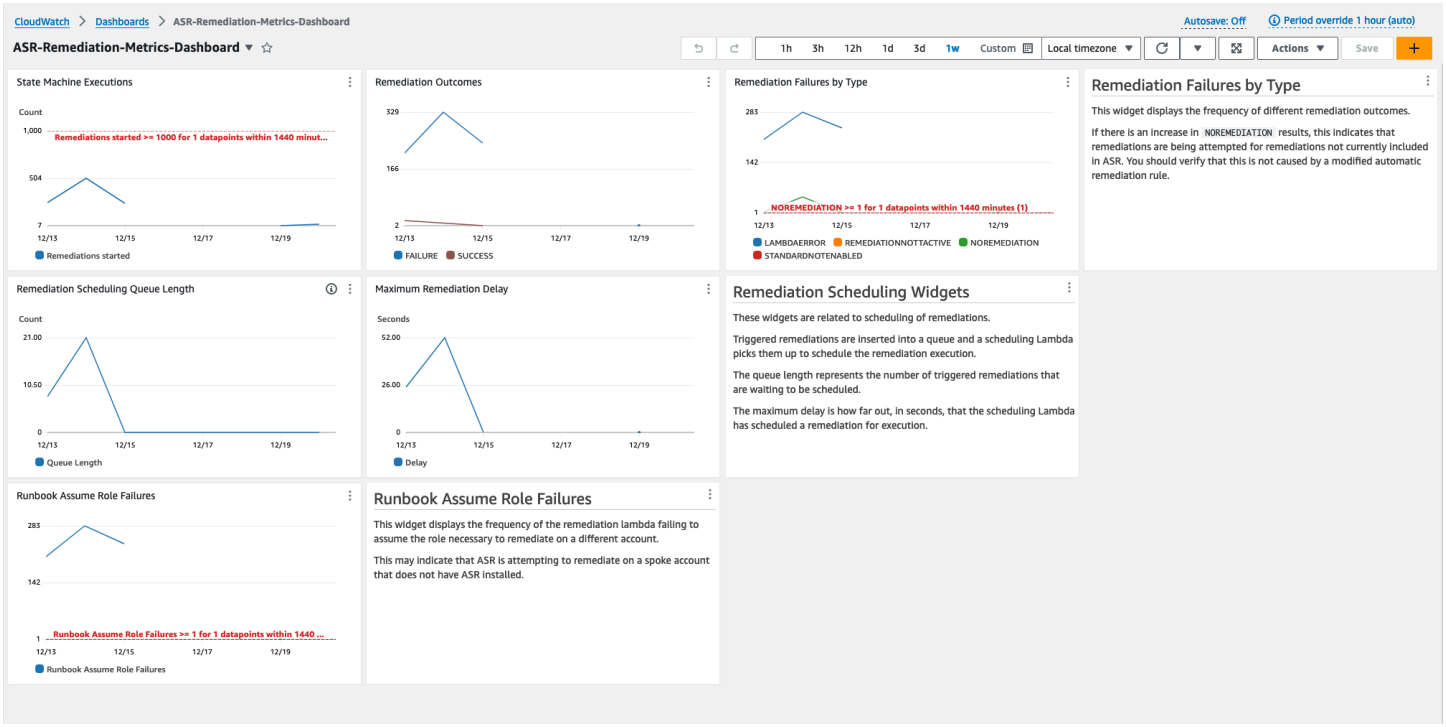
2. Fallos de corrección por tipo = NORREMEDIACIÓN > 0

   a. Se están intentando corregir las correcciones que no están incluidas en el ASR. Esto podría indicar que una regla de eventos se ha modificado para incluir más soluciones de las previstas.

3. Runbook asume errores de rol > 0

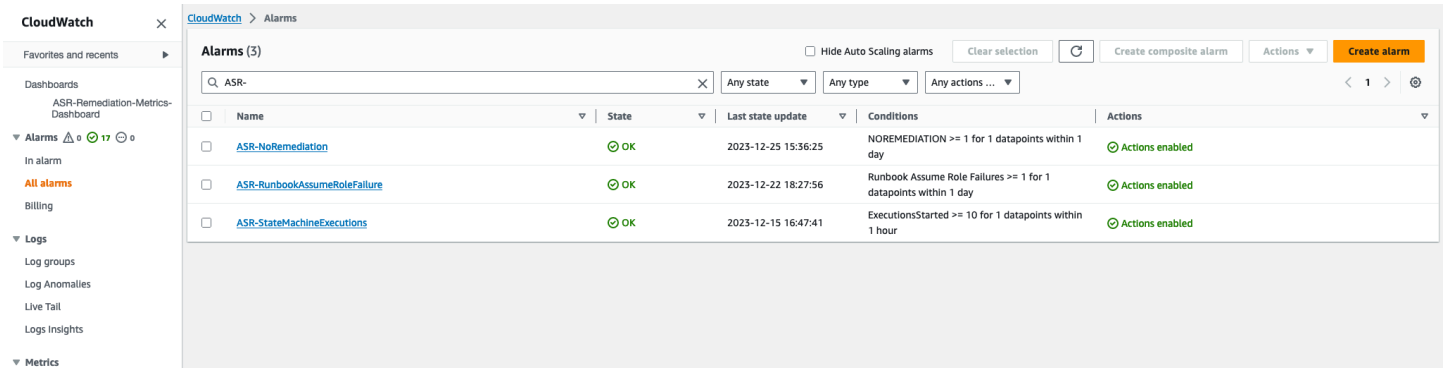
   a. Se están intentando solucionar los problemas en las cuentas o regiones que no cuentan con la solución implementada correctamente. Esto podría indicar que se ha modificado una regla de eventos para incluir más cuentas de las previstas.

Todos los umbrales de alarma se pueden modificar para adaptarlos a las necesidades de implementación individuales.

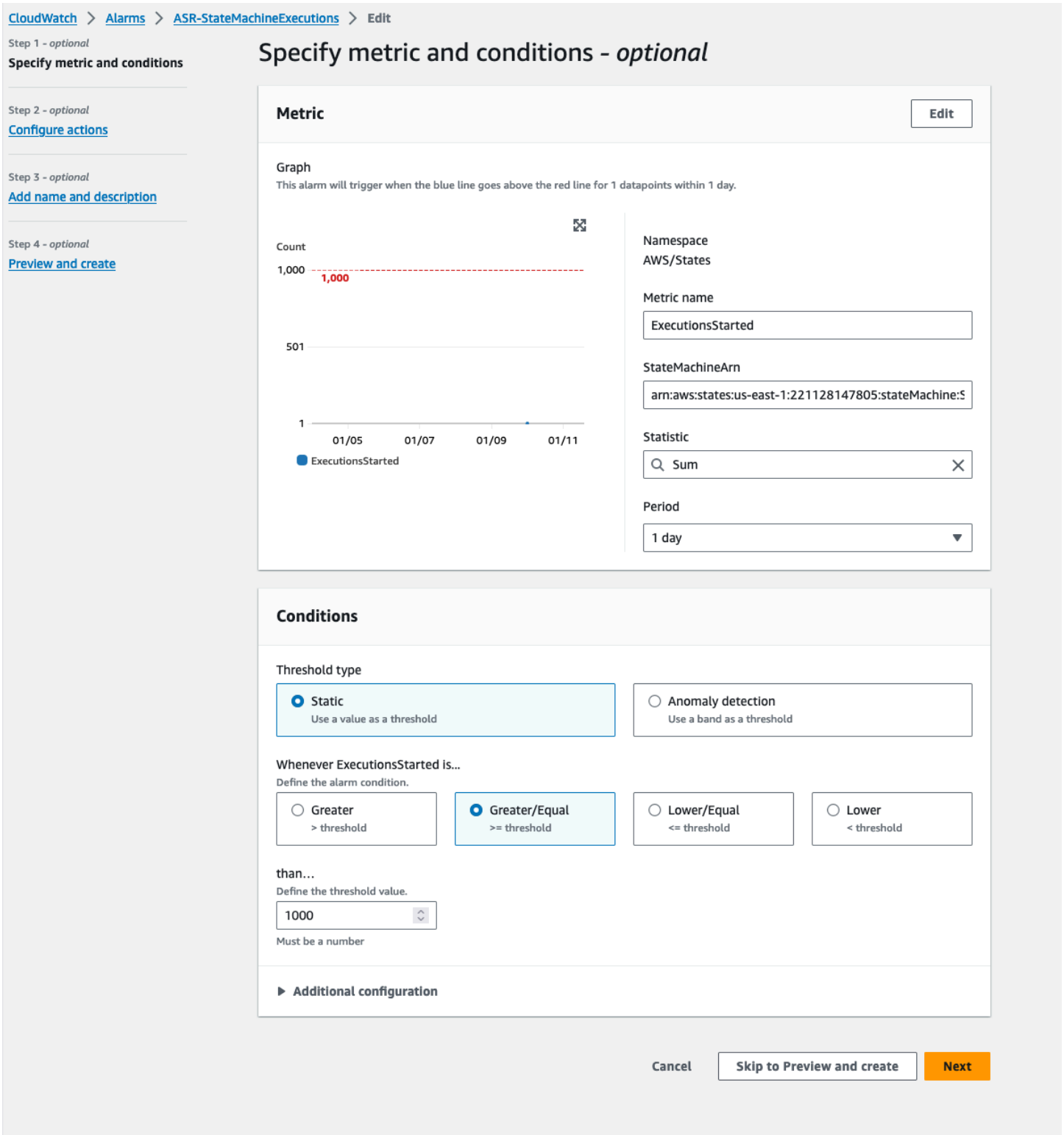


Modificación de los umbrales de alarma

1. Vaya a Amazon CloudWatch → Alarmas → Todas las alarmas.
2. Elija la alarma que desee modificar y, a continuación, seleccione Acciones → Editar.



1. Cambie el umbral al valor deseado y guárdelo.



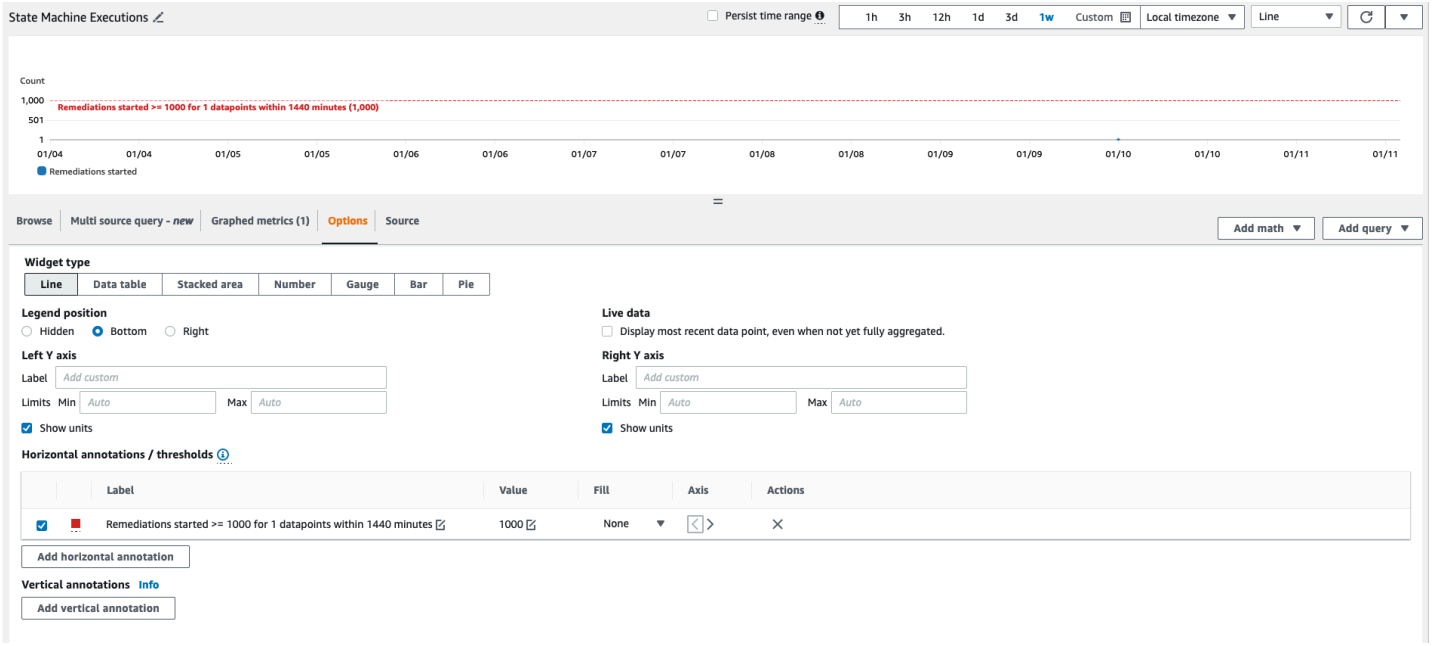
1. Navegue hasta el CloudWatch panel de control para modificar los gráficos para que coincidan con la nueva configuración.

   a. Selecciona los puntos suspensivos en la parte superior derecha del widget correspondiente.

b. Seleccione Editar.

c. Cambie a la pestaña Opciones.

d. Modifique la anotación de la alarma para que coincida con la nueva configuración.



Suscribirse a las notificaciones de alarmas

En la cuenta de administrador, suscríbase al tema de Amazon SNS creado por la pila de administración, SO0111-ASR_Alarm_Topic. Esto le notificará cuando una alarma entre en estado de ALARMA.

Actualización de la solución

Actualización desde versiones anteriores a la v1.4

Si ya implementó la solución con anterioridad a la versión 1.4.x, desinstálela e instale la última versión:

1. Desinstale la solución implementada anteriormente. Consulte Desinstalar la solución.
2. Inicie la plantilla más reciente. Consulte Implementar la solución.

> **Note**
>
> Si va a actualizar de la versión 1.2.1 o anterior a la versión 1.3.0 o posterior, defina Usar un grupo de registros de Orchestrator existente en. `No` Si va a volver a instalar la versión 1.3.0 o posterior, puede seleccionar esta opción. `Yes` Esta opción te permite seguir iniciando sesión en el mismo grupo de registros para las Step Functions de Orchestrator.

Actualización desde la versión 1.4 y versiones posteriores

Si estás actualizando desde la versión 1.4.x, actualiza todas las pilas o de la siguiente manera: StackSets

1. Actualiza la pila en la cuenta de administrador de Security Hub con la plantilla más reciente.
2. En cada cuenta de miembro, actualice los permisos de la plantilla más reciente.
3. En cada cuenta de miembro de todas las regiones en las que esté desplegada actualmente, actualice la pila de miembros a partir de la plantilla más reciente.

Actualización desde la versión 2.0.x

Si está actualizando desde la v2.0.x, actualice a la v2.1.2 o posterior. Si se actualiza a la v2.1.0, se producirá un error en la versión 2.1.1. CloudFormation

Note

- Al actualizar la solución, es posible que sea necesario volver a habilitar manualmente las reglas de corrección automatizadas en la cuenta de administrador. Consulte Habilitar las correcciones totalmente automatizadas.
- Si utiliza el `Reuse Orchestrator Log Group` parámetro para conservar los registros, asegúrese de que esté configurado correctamente durante la actualización de la pila para evitar la recreación de los grupos de registros o la pérdida de la configuración de retención de registros. Consulte Implementar la solución. Si está realizando una actualización de pila a la versión 2.3.0+ desde una versión anterior, elija «no»

Solución de problemas

La resolución de problemas conocidos proporciona instrucciones para mitigar los errores conocidos. Si estas instrucciones no resuelven el problema, Contact AWS Support proporciona instrucciones para abrir un caso de AWS Support para esta solución.

Registros de soluciones

Esta sección incluye información sobre la solución de problemas de esta solución; consulte el menú de navegación de la izquierda para ver los temas.

Esta solución recopila los resultados de los manuales de corrección, que se ejecutan en AWS Systems Manager, y registra el resultado `S00111-ASR` en el grupo CloudWatch Logs de la cuenta de administrador de AWS Security Hub. Hay una transmisión por control por día.

Orchestrator Step Functions registra todas las transiciones de los pasos en el grupo de `S00111-ASR-Orchestrator` CloudWatch registros de la cuenta de administrador de AWS Security Hub. Este registro es una pista de auditoría para registrar las transiciones de estado de cada instancia de Step Functions. Hay un flujo de registro por ejecución de Step Functions.

Ambos grupos de registros se cifran con una clave de administrador de clientes (CMK) de AWS KMS.

La siguiente información de solución de problemas utiliza el `S00111-ASR` grupo de registros. Utilice este registro, así como la consola de AWS Systems Manager Automation, los registros de Automation Executions, la consola Step Function y los registros Lambda para solucionar problemas.

Si se produce un error en una solución, se registrará un mensaje similar al siguiente `S00111-ASR` en el flujo de registro para indicar el estándar, el control y la fecha. Por ejemplo: CIS-2.9-2021-08-12

```
ERROR: a4cbb9bb-24cc-492b-a30f-1123b407a6253: Remediation failed for CIS control
 2.9 in account 123412341234: See Automation Execution output for details (AwsEc2Vpc
 vpc-0e92bbe911cf08acb)
```

Los siguientes mensajes proporcionan detalles adicionales. Este resultado proviene del manual de instrucciones de ASR para el estándar de seguridad y el control. Por ejemplo: ASR-CIS_1.2.0_2.9

```
Step fails when it is Execution complete: verified. Failed to run automation with
 executionId: eecdef79-9111-4532-921a-e098549f5259 Failed :
```

```
{Status=[Failed], Output=[No output available yet because the step is not successfully
 executed], ExecutionId=[eecdef79-9111-4532-921a-e098549f5259]}. Please refer to
 Automation Service Troubleshooting Guide for more diagnosis details.
```

Esta información apunta al error, que en este caso se debió a una automatización secundaria que se estaba ejecutando en la cuenta del miembro. Para solucionar este problema, debe iniciar sesión en la consola de administración de AWS de la cuenta del miembro (del mensaje anterior), ir a AWS Systems Manager, ir a Automation y examinar el resultado del registro para ver el ID `eecdef79-9111-4532-921a-e098549f525` de ejecución.

Resolución de problemas conocidos

- Problema: la implementación de la solución falla y aparece un error que indica que los recursos ya están disponibles en Amazon CloudWatch.

  Solución: compruebe si hay un mensaje de error en la sección de CloudFormation recursos/eventos que indique que los grupos de registros ya existen. Las plantillas de despliegue de ASR permiten reutilizar los grupos de registros existentes. Compruebe que ha seleccionado la reutilización.

- Problema: la solución no se implementa y se produce un error en la pila anidada de un manual de estrategias que impide EventBridge crear una regla

  Solución: Es probable que hayas alcanzado la cuota de EventBridge reglas con la cantidad de libros de jugadas desplegados. Puede evitarlo utilizando las conclusiones de control consolidadas en Security Hub junto con el manual de estrategias de SC de esta solución, implementando solo los manuales de estrategias para los estándares utilizados o solicitando un aumento de la cuota de EventBridge reglas.

- Problema: ejecuto Security Hub en varias regiones de la misma cuenta. Quiero implementar esta solución en varias regiones.

  Solución: Implemente la pila de administración en la misma cuenta y región que el administrador de Security Hub. Instale la plantilla de miembros en cada cuenta y región en la que tenga configurado un miembro de Security Hub. Habilite la agregación en el Security Hub.

- Problema: Inmediatamente después de la implementación, el SO0111-ASR-Orchestrator está fallando en el estado Get Automation Document con un error 502: «`Lambda no ha podido descifrar las variables de entorno porque se ha denegado el acceso al KMS. Compruebe la configuración de las teclas KMS de la función. Excepción de UnrecognizedClientException

KMS: Mensaje de KMS: el token de seguridad incluido en la solicitud no es válido. (Servicio: AWSLambda; código de estado: 502; código de error: KMSAccessDeniedException; ID de solicitud:... `»

Solución: espere unos 10 minutos para que la solución se estabilice antes de ejecutar las correcciones. Si el problema persiste, abra un ticket de soporte o un GitHub problema.

- Problema: he intentado corregir un hallazgo, pero no ha ocurrido nada.

  Solución: consulte las notas del hallazgo para ver los motivos por los que no se ha subsanado. Una causa común es que el hallazgo no tiene una solución automática. En este momento, no hay forma de proporcionar comentarios directos al usuario cuando no existe ninguna solución que no sea a través de las notas. Revise los registros de la solución. Abra CloudWatch los registros en la consola. Busque el grupo de registros SO0111-ASR. CloudWatch Ordene la lista para que aparezcan primero las transmisiones actualizadas más recientemente. Seleccione la secuencia de registro para la búsqueda que intentó ejecutar. Ahí debería encontrar cualquier error. Algunos de los motivos del error podrían ser: la falta de coincidencia entre buscar el control y el control de remediación, la subsanación entre cuentas (aún no se admite) o el hecho de que la constatación ya se haya subsanado. Si no puede determinar el motivo del error, recopile los registros y abra un ticket de soporte.

- Problema: Tras iniciar una corrección, el estado de la consola de Security Hub no se ha actualizado.

  Solución: la consola de Security Hub no se actualiza automáticamente. Actualice la vista actual. El estado del hallazgo debería actualizarse. Es posible que la conclusión tarde varias horas en pasar de ser rechazada a aprobada. Los resultados se crean a partir de los datos de eventos enviados por otros servicios, como AWS Config, a AWS Security Hub. El tiempo que transcurre hasta que se vuelva a evaluar una regla depende del servicio subyacente. Si esto no resuelve el problema, consulte la resolución anterior para «`Intenté corregir una constatación, pero no ocurrió nada. `»

- Problema: la función paso a paso de Orchestrator falla al obtener el estado del documento de automatización: se produjo un error (AccessDenied) al llamar a la AssumeRole operación.

  Solución: la plantilla de miembros no se ha instalado en la cuenta de miembro en la que ASR intenta corregir un hallazgo. Siga las instrucciones para implementar la plantilla de miembros.

- Problema: el runbook de Config.1 falla porque ya existe la grabadora o el canal de entrega.

Solución: inspeccione detenidamente la configuración de AWS Config para asegurarse de que la configuración está correctamente configurada. En algunos casos, la corrección automática no puede corregir la configuración de AWS Config existente.

- Problema: la corrección se ha realizado correctamente, pero devuelve el mensaje `"No output available yet because the step is not successfully executed."`

  Solución: se trata de un problema conocido en esta versión, por el que algunos manuales de corrección no muestran ninguna respuesta. Los manuales de corrección fallarán correctamente y, si no funcionan, indicarán la solución.

- Problema: La resolución falló y envió un seguimiento de la pila.

  Solución: En ocasiones, perdemos la oportunidad de gestionar una condición de error que provoca un seguimiento de la pila en lugar de un mensaje de error. Intente solucionar el problema a partir de los datos de rastreo. Abre un ticket de soporte si necesitas ayuda.

- Problema: No se pudo eliminar la pila de la versión 1.3.0 en el recurso Custom Action.

  Solución: es posible que no se pueda eliminar la plantilla de administración si se elimina la acción personalizada. Se trata de un problema conocido que se solucionará en la próxima versión. Si esto ocurre:

  a. Inicie sesión en la consola de administración de AWS Security Hub.
  b. En la cuenta de administrador, vaya a Configuración.
  c. Selecciona la pestaña Acciones personalizadas
  d. Elimine manualmente la entrada Remediar con ASR.
  e. Vuelva a eliminar la pila.

- Problema: Tras volver a implementar la pila de administración, la función Step está fallando. `AssumeRole`

  Solución: Al volver a implementar la pila de administradores, se rompe la conexión de confianza entre la función de administrador en la cuenta de administrador y la función de miembro en las cuentas de miembro. Debes volver a distribuir la pila de funciones de los miembros en todas las cuentas de los miembros.

- Problema: las correcciones de CIS 3.x no aparecen `PASSED` después de más de 24 horas.

  Solución: Esto ocurre con frecuencia si no tiene suscripciones al tema de `SO0111-ASR_LocalAlarmNotification` SNS en la cuenta del miembro.

Problemas con soluciones específicas

La SSLBucket política de configuración falla y se produce un AccessDenied error

Controles asociados: AWS FSBP v1.0.0 S3.5, PCI v3.2.1 PCI.S3.5, CIS v1.4.0 2.1.2, SC v2.0.0 S3.5

Problema: la política establecida SSLBucket AccessDenied falla y se produce el siguiente error:

Se produjo un error (AccessDenied) al llamar a la PutBucketPolicy operación: acceso denegado

Si se ha activado la configuración Bloquear el acceso público para un depósito, los intentos de establecer una política de depósito que incluya sentencias que permitan el acceso público fallarán y se mostrará este error. Se puede alcanzar este estado poniendo una política de compartimentos que contenga dichas declaraciones y, a continuación, habilitando el bloqueo de acceso público para ese depósito.

La corrección ConfigureS3 BucketPublicAccessBlock (controles asociados: AWS FSBP v1.0.0 S3.2, PCI v3.2.1 PCI.S3.2, CIS v1.4.0 2.1.5.2, SC v2.0.0 S3.2) también puede poner un bucket en este estado porque establece la configuración de bloqueo de acceso público sin cambiar la política del bucket.

La SSLBucket política de conjunto añade una declaración a la política de bucket para denegar las solicitudes que no utilizan SSL. No modifica las demás declaraciones de la política, por lo que, si hay declaraciones que permiten el acceso público, la solución fallará al intentar incluir la política de bucket modificada que aún incluye esas declaraciones.

Solución: modifique la política de compartimentos para eliminar las declaraciones que permiten el acceso público que entren en conflicto con la configuración de bloquear el acceso público del depósito.

PutS3 falla BucketPolicyDeny

Controles asociados: AWS FSBP v1.0.0 S3.6, NIST.800-53.r5 CA-9 (1), NiST.800-53.r5 CM-2

ProblemaBucketPolicyDeny : el PuTs3 con el siguiente error:

```
Unable to create an explicit deny statement for {bucket_name}.
```

Si los principios de todas las políticas del segmento de destino son «*», la solución no puede añadir la política de denegación al grupo de destino, ya que bloquearía todas las acciones del grupo de destino para todos los principales.

Solución: modifique la política de compartimentos para permitir acciones en cuentas específicas en lugar de utilizar los principios «*» y restrinja las acciones denegadas.

¿Cómo deshabilitar la solución

En caso de que se produzca un incidente, es posible que necesite deshabilitar la solución sin eliminar ninguna parte de la infraestructura. Estos escenarios detallan cómo deshabilitar los diferentes componentes de la solución.

Escenario 1: deshabilitar la corrección automática para un solo control.

1. Navegue hasta EventBridge en la CloudFormation consola de AWS.
2. Seleccione Reglas en la barra lateral.
3. Seleccione el bus de eventos predeterminado y busque el control que desee deshabilitar.
4. Seleccione la regla y pulse el botón Desactivar.

Escenario 2: deshabilitar la corrección automática para todos los controles.

1. Navegue hasta EventBridge la consola.
2. Selecciona Reglas en la barra lateral.
3. Selecciona el bus de eventos «predeterminado» y selecciona todas las reglas que aparecen a continuación.
4. Selecciona el botón «Desactivar». Tenga en cuenta que es posible que tenga que hacer esto para varias páginas de reglas.

Escenario 3: deshabilitar la corrección manual para una cuenta

1. Navegue hasta EventBridge la consola.
2. Selecciona Reglas en la barra lateral.
3. Seleccione el bus de eventos «predeterminado» y busque «Remediate_with_ASR_» CustomAction
4. Seleccione la regla y pulse el botón «Desactivar».

Contacto con Support

Si cuenta con AWS Developer Support, AWS Business Support o AWS Enterprise Support, puede utilizar el Centro de soporte para obtener asistencia de expertos con esta solución. En las siguientes secciones, encontrará instrucciones.

Cree un caso

1. Inicie sesión en Support Center.
2. Seleccione Crear caso.

¿Cómo podemos ayudar?

1. Elija Técnico.
2. Para el servicio, seleccione Soluciones.
3. En Categoría, seleccione Otras soluciones.
4. En Gravedad, seleccione la opción que mejor se adapte a su caso de uso.
5. Al introducir el servicio, la categoría y la gravedad, la interfaz rellena los enlaces a las preguntas de solución de problemas más frecuentes. Si no puede resolver su pregunta con estos enlaces, seleccione Siguiente paso: información adicional.

Información adicional

1. En Asunto, introduce un texto que resuma tu pregunta o problema.
2. En Descripción, describe el problema en detalle.
3. Selecciona Adjuntar archivos.
4. Adjunte la información que Support necesita para procesar la solicitud.

Ayúdenos a resolver su caso más rápido

1. Introduzca la información solicitada.
2. Elija Siguiente paso: Resuelva ahora o póngase en contacto con nosotros.

Resuelva ahora o póngase en contacto con nosotros

1. Revise las soluciones Solve now.
2. Si no puede resolver su problema con estas soluciones, elija Contactar con nosotros, introduzca la información solicitada y pulse Enviar.

Desinstalar la solución

Utilice el siguiente procedimiento para desinstalar la solución con la consola de administración de AWS.

V1.0.0-V1.2.1

Para las versiones v1.0.0 a v1.2.1, utilice Service Catalog para desinstalar los manuales de estrategias del CIS FSBP. and/or Con la versión 1.3.0, Service Catalog ya no se utiliza.

1. Inicie sesión en la CloudFormation consola de AWS y vaya a la cuenta principal de Security Hub.
2. Elija Service Catalog para finalizar cualquier manual aprovisionado y eliminar cualquier grupo de seguridad, rol o usuario.
3. Elimine la `CISPermissions.template` plantilla de radios de las cuentas de los miembros de Security Hub.
4. Elimine la `AFSBPMemberStack.template` plantilla radial de las cuentas de administrador y miembro de Security Hub.
5. Navegue hasta la cuenta principal de Security Hub, seleccione la pila de instalación de la solución y, a continuación, elija Eliminar.

> **Note**
>
> CloudWatch Se conservan los registros de los grupos de registros. Recomendamos conservar estos registros según lo exige la política de retención de registros de su organización.

V1.3.x

1. Elimine el de cada `automated-security-response-member.template` cuenta de miembro.
2. Elimine el `automated-security-response-admin.template` de la cuenta de administrador.

> **Note**
>
> Es probable que no se pueda eliminar la plantilla de administración en la versión 1.3.0 si se elimina la acción personalizada. Se trata de un problema conocido que se solucionará en la próxima versión. Siga las instrucciones siguientes para solucionar este problema:
>
> 1. Inicie sesión en la consola de administración de AWS Security Hub.
> 2. En la cuenta de administrador, vaya a Configuración.
> 3. Selecciona la pestaña Acciones personalizadas.
> 4. Elimine manualmente la entrada Remediar con ASR.
> 5. Vuelva a eliminar la pila.

V1.4.0 y versiones posteriores

Implementación de Stack

1. Elimine el `automated-security-response-member.template` de la cuenta de cada miembro.
2. Elimine el `automated-security-response-admin.template` de la cuenta de administrador.

StackSet Implementación

Para cada una de ellas StackSet, elimina las pilas y, a continuación, quita las StackSet pilas siguiendo el orden inverso al de despliegue.

Tenga en cuenta que las funciones de IAM del `automated-security-response-member-roles.template` se conservan incluso si se elimina la plantilla. Esto es para que las soluciones que utilizan estas funciones sigan funcionando. Estas funciones del SO0111-* se pueden eliminar manualmente después de comprobar que ya no las utilizan las soluciones activas, como CloudTrail el registro o la supervisión mejorada de RDS. CloudWatch

Guía del administrador

Activación y desactivación de partes de la solución

Como administrador de la solución, tiene los siguientes controles sobre las funcionalidades de la solución que están habilitadas.

Dónde se despliegan los grupos de miembros y funciones de los miembros:

- La pila de administradores solo podrá iniciar correcciones (mediante acciones personalizadas o EventBridge reglas totalmente automatizadas) en las cuentas en las que se hayan desplegado las pilas de miembros y roles de miembros, con el número de cuenta de administrador indicado como valor de parámetro.
- Para eximir por completo a las cuentas o regiones del control de la solución, no distribuya los grupos de miembros o roles de miembros en esas cuentas o regiones.

Configuración de agregación de búsqueda de cuentas y regiones en Security Hub:

- El grupo de administradores solo podrá iniciar las correcciones (mediante acciones personalizadas o EventBridge reglas totalmente automatizadas) en caso de que los hallazgos lleguen a la cuenta de administrador y a la región.
- Para eximir completamente a las cuentas o regiones del control de la solución, no incluyas esas cuentas o regiones para enviar las conclusiones a la misma cuenta de administrador y a la misma región en la que está desplegada la pila de administradores.

Qué pilas anidadas estándar se implementan:

- El equipo de administradores solo podrá iniciar correcciones (mediante acciones personalizadas o EventBridge reglas totalmente automatizadas) en los controles que tengan un manual de control implementado en la cuenta del miembro objetivo y en la región. Los despliega el grupo de miembros de cada norma.
- La pila de administradores solo podrá iniciar correcciones totalmente automatizadas mediante EventBridge reglas para los controles que tengan las reglas implementadas por la pila de administración para ese estándar. Se implementan en la cuenta de administrador.
- Para simplificar, te recomendamos implementar estándares de forma coherente en tus cuentas de administrador y de miembro. Si le interesan AWS FSBP y CIS v1.2.0, implemente esas dos

pilas de administración anidadas en la cuenta de administrador e implemente esas dos pilas de miembros anidadas en cada cuenta de miembro y región.

Qué manuales de control están implementados en cada pila de miembros anidada:

- El grupo de administradores solo podrá iniciar correcciones (mediante acciones personalizadas o EventBridge reglas totalmente automatizadas) para los controles que tengan un manual de control implementado en la cuenta del miembro objetivo y en la región por grupo de miembros para cada estándar.
- Para ejercer un control más preciso sobre qué controles están habilitados para un estándar en particular, cada pila anidada de un estándar tiene parámetros para los manuales de control que se utilizan. Establezca el parámetro de un control en el valor «NO disponible» para anular la implementación de ese manual de controles.

Parámetros de SSM para activar y desactivar los estándares:

- La pila de administradores solo podrá iniciar correcciones (mediante acciones personalizadas o EventBridge reglas totalmente automatizadas) para los estándares que estén habilitados mediante el parámetro SSM implementado por la pila de administración estándar.
- <standard_name><standard_version>Para deshabilitar un estándar, defina el valor del parámetro SSM con la ruta «/Solutions/SO0111///status» en «No».

Ejemplo de notificaciones de SNS

Cuando se inicia una remediación

```
{
 "severity": "INFO",
 "message": "00000000-0000-0000-0000-000000000000: Remediation queued for SC control
 RDS.13 in account 111111111111",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
```

```
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

Cuando una remediación se realiza correctamente

```
{
 "severity": "INFO",
 "message": "00000000-0000-0000-0000-000000000000: Remediation succeeded for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

Cuando se produce un error en una corrección

```
{
 "severity": "ERROR",
 "message": "00000000-0000-0000-0000-000000000000: Remediation failed for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
```

```
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

Usa la solución

Este es un tutorial que lo guiará durante la primera implementación de ASR. Comenzará con los requisitos previos para implementar la solución y terminará con una corrección de los ejemplos encontrados en una cuenta de miembro.

Tutorial: Introducción a la respuesta de seguridad automatizada en AWS

Este es un tutorial que lo guiará durante su primera implementación. Comenzará con los requisitos previos para implementar la solución y terminará con la corrección de los ejemplos encontrados en una cuenta de miembro.

Prepare las cuentas

Para demostrar las capacidades de corrección de la solución entre cuentas y regiones, en este tutorial se utilizarán dos cuentas. También puede implementar la solución en una sola cuenta.

En los siguientes ejemplos se utilizan cuentas `111111111111` y `222222222222` se muestra la solución. `111111111111`será la cuenta de administrador y `222222222222` será la cuenta de miembro. Configuraremos la solución para corregir los hallazgos de recursos en las regiones `us-east-1` y`us-west-2`.

La siguiente tabla es un ejemplo que ilustra las medidas que tomaremos para cada paso en cada cuenta y región.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
`111111111111`	Administrador	Ninguno	Ninguno
`222222222222`	Miembro	Ninguno	Ninguno

La cuenta de administrador es la cuenta que realizará las acciones de administración de la solución, es decir, iniciar las correcciones manualmente o habilitar la remediación totalmente automatizada con reglas. EventBridge Esta cuenta también debe ser la cuenta de administrador delegado de Security Hub para todas las cuentas en las que desee corregir los hallazgos, pero no tiene por qué ser ni

debe ser la cuenta de administrador de AWS Organizations de la organización de AWS a la que pertenecen sus cuentas.

Habilitar AWS Config

Consulte la siguiente documentación:

- Documentación de AWS Config
- Precios de AWS Config
- Habilitación de AWS Config

Habilite AWS Config en ambas cuentas y regiones. Esto conllevará cargos.

> **Important**
>
> Asegúrese de seleccionar la opción «Incluir recursos globales (por ejemplo, recursos de AWS IAM)». Si no selecciona esta opción al habilitar AWS Config, no verá los resultados relacionados con los recursos globales (por ejemplo, los recursos de AWS IAM)

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Habilitar AWS Config	Habilitar AWS Config
222222222222	Miembro	Habilitar AWS Config	Habilitar AWS Config

Habilitar el centro de seguridad de AWS

Consulte la siguiente documentación:

- Documentación de AWS Security Hub
- Precios de AWS Security Hub
- Habilitación de AWS Security Hub

Habilite AWS Security Hub en ambas cuentas y regiones. Esto conllevará cargos.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Habilitar AWS Security Hub	Habilitar AWS Security Hub
222222222222	Miembro	Habilitar AWS Security Hub	Habilitar AWS Security Hub

Habilite los hallazgos de control consolidados

Revise la siguiente documentación:

- Generación y actualización de los resultados de control

Para los fines de este tutorial, demostraremos el uso de la solución con la función de hallazgos de control consolidados de AWS Security Hub habilitada, que es la configuración recomendada. En las particiones que no admitan esta función en el momento de escribir este artículo, tendrá que implementar los manuales específicos del estándar en lugar del SC (Security Control).

Habilite los resultados de control consolidados tanto en las cuentas como en las dos regiones.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Habilite los hallazgos de control consolida dos	Habilite los hallazgos de control consolida dos
222222222222	Miembro	Habilite los hallazgos de control consolida dos	Habilite los hallazgos de control consolida dos

Es posible que los hallazgos tarden algún tiempo en generarse con la nueva función. Puede continuar con el tutorial, pero no podrá corregir los hallazgos generados sin la nueva función. Los

hallazgos generados con la nueva función se pueden identificar mediante el valor `security-control/<control_id>` del `GeneratorId` campo.

Configure la agregación de búsquedas entre regiones

Consulte la siguiente documentación:

- Agregación entre regiones
- Habilitar la agregación entre regiones

Configura la agregación de búsqueda de us-west-2 a us-east-1 en ambas cuentas.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Configurar la agregación desde us-west-2	Ninguno
222222222222	Miembro	Configurar la agregación desde us-west-2	Ninguno

Es posible que los hallazgos tarden algún tiempo en propagarse a la región de agregación. Puede continuar con el tutorial, pero no podrá corregir los hallazgos de otras regiones hasta que comiencen a aparecer en la región de agregación.

Designe una cuenta de administrador de Security Hub

Revise la siguiente documentación:

- Administración de cuentas en AWS Security Hub
- Administrar las cuentas de los miembros de la
- Administrar las cuentas de los miembros mediante invitación

En el ejemplo anterior, utilizaremos el método de invitación manual. Para un conjunto de cuentas de producción, recomendamos gestionar la administración delegada de Security Hub a través de AWS Organizations.

Desde la consola de AWS Security Hub en la cuenta de administrador (111111111111), invite a la cuenta miembro (222222222222) a aceptar la cuenta de administrador como administrador delegado de Security Hub. Desde la cuenta del miembro, acepte la invitación.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Invita a la cuenta de miembro	Ninguno
222222222222	Miembro	Acepta la invitación	Ninguno

Es posible que los resultados tarden algún tiempo en propagarse a la cuenta de administrador. Puedes continuar con el tutorial, pero no podrás corregir los hallazgos de las cuentas de los miembros hasta que empiecen a aparecer en la cuenta de administrador.

Crea los roles para los permisos autogestionados StackSets

Revise la siguiente documentación:

- AWS CloudFormation StackSets
- Otorgue permisos autogestionados

Vamos a implementar CloudFormation pilas en varias cuentas, por lo que las usaremos. StackSets No podemos usar permisos administrados por el servicio porque la pila de administradores y la pila de miembros tienen pilas anidadas, que no son compatibles con el servicio, por lo que debemos usar permisos autogestionados.

Implemente las pilas para obtener permisos básicos para las operaciones. StackSet En el caso de las cuentas de producción, es posible que desee limitar los permisos de acuerdo con la documentación sobre las «opciones de permisos avanzadas».

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Implemente el conjunto de funciones StackSet de administrador Implemente la pila StackSet de funciones de ejecución	Ninguno
222222222222	Miembro	Implemente la pila StackSet de funciones de ejecución	Ninguno

Cree los recursos inseguros que generarán hallazgos de ejemplo

Revise la siguiente documentación:

- Referencia de controles de Security Hub
- Controles de AWS Lambda

El siguiente recurso de ejemplo con una configuración insegura para demostrar una solución. El ejemplo de control es Lambda.1: Las políticas de funciones de Lambda deberían prohibir el acceso público.

> **Important**
>
> Crearemos intencionalmente un recurso con una configuración insegura. Revise la naturaleza del control y evalúe usted mismo el riesgo de crear un recurso de este tipo en su entorno. Tenga en cuenta cualquier herramienta de la que disponga su organización para detectar y denunciar dichos recursos y solicite una excepción, si procede. Si el control de ejemplo que hemos seleccionado no es adecuado para usted, seleccione otro control compatible con la solución.

En la segunda región de la cuenta de miembro, diríjase a la consola de AWS Lambda y cree una función en el último entorno de ejecución de Python. En Configuración → Permisos, añada una declaración de política que permita invocar la función desde la URL sin autenticación.

Confirme en la página de la consola que la función permite el acceso público. Una vez que la solución solucione este problema, compare los permisos para confirmar que se ha revocado el acceso público.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
`111111111111`	Administrador	Ninguno	Ninguno
`222222222222`	Miembro	Ninguno	Cree una función Lambda con una configuración insegura

Es posible que AWS Config tarde algún tiempo en detectar la configuración insegura. Puede continuar con el tutorial, pero no podrá corregir el hallazgo hasta que Config lo detecte.

Cree grupos de CloudWatch registros para los controles relacionados

Revise la siguiente documentación:

- Supervisión de archivos de CloudTrail registro con Amazon CloudWatch Logs
- CloudTrail controles

CloudTrail Los diversos controles compatibles con la solución requieren que haya un grupo de CloudWatch registros que sea el destino de una región múltiple CloudTrail. En el siguiente ejemplo, crearemos un grupo de registros de marcadores de posición. En el caso de las cuentas de producción, debe configurar correctamente CloudTrail la integración con CloudWatch los registros.

Cree un grupo de registros en cada cuenta y región con el mismo nombre, por ejemplo:`asr-log-group`.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Creación de un grupo de registros	Crear un grupo de registro
222222222222	Miembro	Creación de un grupo de registros	Crear un grupo de registro

Implemente la solución en las cuentas de tutoriales

Reúna los tres Amazon S3 URLs para la pila de roles de administrador, miembro y miembro.

Implemente la pila de administración

View template

automa

security-response-admin.template

En la cuenta de administrador, vaya a la CloudFormation consola e implemente la pila de administración en la región de agregación de búsqueda del Security Hub.

Elija No el valor de todos los parámetros para cargar las pilas de administración anidadas, excepto la pila «SC» o «Security Control». Esta pila contiene los recursos para las conclusiones de control consolidadas que hemos configurado en nuestras cuentas.

Elija No reutilizar el grupo de registros de Orchestrator, a menos que haya implementado esta solución anteriormente en esta cuenta y región.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Implemente la pila de administración	Ninguno
222222222222	Miembro	Ninguno	Ninguno

Espere a que la pila de administración complete la implementación antes de continuar para poder crear una relación de confianza entre las cuentas de los miembros y la cuenta de administrador.

Implemente la pila de miembros

View template

automa

security-response-member.plantilla

En la cuenta de administrador, diríjete a la CloudFormation StackSets consola e implementa el grupo de miembros en cada cuenta y región. Usa los roles de StackSets administración y ejecución creados en este tutorial.

Introduzca el nombre del grupo de registros que creó como valor del parámetro del nombre del grupo de registros.

Elija No el valor de todos los parámetros para cargar las pilas de miembros anidadas, excepto la pila «SC» o «control de seguridad». Esta pila contiene los recursos para las conclusiones de control consolidadas que hemos configurado en nuestras cuentas.

Introduzca el ID de la cuenta de administrador como valor del parámetro del número de cuenta de administrador. En nuestro ejemplo, esto es111111111111.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Despliegue el miembro o confirme StackSet la pila de miembros desplegada	Confirme que la pila de miembros esté despleg
222222222222	Miembro	Confirme que la pila de miembros está despleg	Confirme que la pila de miembros está despleg

Implemente la pila de roles de los miembros

automated-security-response-memberbotón de plantilla -roles.template -roles.template automated-security-response-member

En la cuenta de administrador, dirígete a la CloudFormation StackSets consola e implementa el grupo de miembros en cada cuenta. Usa los roles de StackSets administración y ejecución creados en este tutorial. Introduzca el ID de la cuenta de administrador como valor del parámetro del número de cuenta de administrador. En nuestro ejemplo, esto es111111111111.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Despliegue el miembro o confirme StackSet la pila de miembros desplegada	Ninguno
222222222222	Miembro	Confirme que la pila de miembros esté despleg	Ninguno

Puede continuar, pero no podrá corregir los hallazgos hasta que CloudFormation StackSets finalice la implementación.

Suscríbase al tema SNS

Actualizaciones de remediación

Tema - {https---us-east-1-console-aws-amazon-com-sns-v3- home-region-us-east -1— -US-East-1-221128147805-SO0111-ASR-topic} [topic-arn-aws-snsSO0111-ASR_topic]

En la cuenta de administrador, suscríbase al tema de Amazon SNS creado por la pila de administradores. Esto le notificará cuando se inicien las correcciones y cuándo se hayan realizado correctamente o no.

Alarmas

Tema - {https---us-east-1-console-aws-amazon-com-sns-v3- home-region-us-east -1— -US-East-1-221128147805-so0111-asr-alarm-topic} [topic-arn-aws-snsSO0111-asr_alarm_topic]

En la cuenta de administrador, suscríbase al tema de Amazon SNS creado por la pila de administradores. Esto le notificará cuando se inicien las alarmas métricas.

Corrija los resultados de los ejemplos

En la cuenta de administrador, navegue hasta la consola de Security Hub y busque el recurso con una configuración insegura que creó como parte de este tutorial.

Esto puede hacerse de varias maneras:

1. En las particiones que admiten la función de resultados del control consolidado, hay una página denominada «Controles» que permite localizar el hallazgo mediante el identificador del control consolidado.
2. En la página «Normas de seguridad», puede localizar el control según el estándar al que pertenece.
3. Puede ver todos los resultados en la página «Hallazgos» y buscar por atributo.

El identificador de control consolidado para la función Lambda pública que creamos es Lambda.1.

Inicie la corrección

Seleccione la casilla de verificación situada a la izquierda del hallazgo relacionado con el recurso que creamos. En el menú desplegable «Acciones», selecciona «Remediar con ASR». Verás una notificación en la que se indica que el hallazgo se ha enviado a Amazon EventBridge.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Inicie la remediación	Ninguno
222222222222	Miembro	Ninguno	Ninguno

Confirme que la corrección resolvió el hallazgo

Deberías recibir dos notificaciones de SNS. La primera indicará que se ha iniciado una corrección y la segunda indicará que la remediación se ha realizado correctamente. Tras recibir la segunda notificación, diríjase a la consola Lambda de la cuenta del miembro y confirme que se ha revocado el acceso público.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Ninguno	Ninguno
222222222222	Miembro	Ninguno	Confirme que la corrección se ha realizado correctamente

Rastree la ejecución de la corrección

Para comprender mejor cómo funciona la solución, puede rastrear la ejecución de la corrección.

EventBridge regla

En la cuenta de administrador, busque una EventBridge regla llamada CustomActionRemediate_with_ASR_. Esta regla coincide con el hallazgo que enviaste desde Security Hub y lo envía a Orchestrator Step Functions.

Ejecución de Step Functions

En la cuenta de administrador, busque las AWS Step Functions denominadas "SO0111-ASR-Orchestrator». Esta función de pasos llama al documento de automatización de SSM en la cuenta y región de destino. Puede rastrear la ejecución de la corrección en el historial de ejecución de este AWS Step Functions.

Automatización de SSM

En la cuenta de miembro, vaya a la consola de SSM Automation. Encontrará dos ejecuciones de un documento denominado «ASR-SC_2.0.0_Lambda.1" y una ejecución de un documento denominado «ASR-». RemoveLambdaPublicAccess

La primera ejecución es desde la función de pasos del orquestador en la cuenta de destino. La segunda ejecución se produce en la región de destino, que puede no ser la región en la que se originó el hallazgo. La ejecución final es la corrección que revoca la política de acceso público de la Función Lambda.

CloudWatch Grupo de registros

En la cuenta de administrador, vaya a la consola de CloudWatch registros y busque un grupo de registros denominado "SO0111-ASR». Este grupo de registros es el destino de los registros de alto nivel de las Step Functions de Orchestrator.

Habilite las correcciones totalmente automatizadas

El otro modo de funcionamiento de la solución consiste en corregir automáticamente los hallazgos a medida que llegan a Security Hub.

Confirme que no tiene recursos a los que se pueda aplicar accidentalmente este hallazgo

Al habilitar las correcciones automáticas, se iniciarán las correcciones en todos los recursos que coincidan con el control que habilite (Lambda.1).

> **Important**
>
> Confirme que quiere que se revoque este permiso a todas las funciones Lambda públicas incluidas en el ámbito de la solución. El alcance de las correcciones totalmente automatizadas no se limitará a la función que haya creado. La solución solucionará este control si se detecta en alguna de las cuentas o regiones en las que esté instalado.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Confirma que no hay ninguna función pública deseada	Confirme que no haya ninguna función pública deseada
222222222222	Miembro	Confirme que no haya ninguna función pública deseada	Confirme que no haya ninguna función pública deseada

Habilite la regla

En la cuenta de administrador, busque una EventBridge regla denominada AutoTriggerSC_2.0.0_Lambda.1_ y habilítela.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Habilite las reglas de remediación automatizadas	Ninguno
222222222222	Miembro	Ninguno	Ninguno

Configure el recurso

En la cuenta del miembro, vuelva a configurar la función Lambda para permitir el acceso público.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Ninguno	Ninguno
222222222222	Miembro	Ninguno	Configurar la función Lambda para permitir el acceso público

Confirme que la corrección resolvió el hallazgo

Es posible que Config tarde algún tiempo en volver a detectar la configuración insegura. Deberías recibir dos notificaciones de SNS. La primera indicará que se ha iniciado una reparación. La segunda indicará que la remediación se ha realizado correctamente. Tras recibir la segunda notificación, diríjase a la consola Lambda de la cuenta del miembro y confirme que se ha revocado el acceso público.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Habilite las reglas de remediación automatizadas	Ninguno
222222222222	Miembro	Ninguno	Confirme que la corrección se ha realizado correctamente

Limpieza

Elimine los recursos de ejemplo

En la cuenta de miembro, elimine la función Lambda de ejemplo que creó.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Ninguno	Ninguno
222222222222	Miembro	Ninguno	Eliminar la función Lambda de ejemplo

Elimine la pila de administración

En la cuenta de administrador, elimina la pila de administración.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Elimina la pila de administración	Ninguno

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
222222222222	Miembro	Ninguno	Ninguno

Elimina la pila de miembros

En la cuenta de administrador, elimina el miembro StackSet.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Eliminar el miembro StackSet Confirme que se ha eliminado la pila de	Confirme que se ha eliminado la pila de
222222222222	Miembro	Confirme que se ha eliminado la pila de	Confirme que se ha eliminado la pila de

Elimine la pila de roles de los miembros

En la cuenta de administrador, elimina los roles de los miembros StackSet.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Elimine los roles de los miembros StackSet Confirme que se ha eliminado la pila de roles de recordar	Ninguno

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
222222222222	Miembro	Confirme que la pila de roles de los miembros se	Ninguno

Elimine los roles retenidos

En cada cuenta, elimine las funciones de IAM retenidas.

Importante: Estas funciones se conservan para las correcciones que requieren una función para que la remediación siga funcionando (por ejemplo, el registro de flujos de VPC). Confirme que no necesita que ninguna de estas funciones siga funcionando antes de eliminarlas.

Elimine todos los roles con el prefijo SO0111-.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Eliminar los roles retenidos	Ninguno
222222222222	Miembro	Eliminar los roles retenidos	Ninguno

Programa la eliminación de las claves KMS retenidas

Tanto las pilas de administradores como las de miembros crean y conservan una clave KMS. Si conserva estas claves, incurrirá en gastos.

Estas claves se conservan para que pueda acceder a cualquier recurso cifrado por la solución. Confirme que no las necesita antes de programar su eliminación.

Identifique las claves implementadas por la solución mediante los alias creados por la solución o a partir del CloudFormation historial. Prográmelas para que se eliminen.

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Identifique y programe la eliminación de la clave de administr ación Identifique y programe la eliminación de la clave del miembro	Identifique y programe la eliminación de la clave del miembro
222222222222	Miembro	Identifique y programe la eliminación de la clave del miembro	Identifique y programe la eliminación de la clave del miembro

Elimine las pilas de permisos autogestionados StackSets

Elimine las pilas creadas para permitir los permisos autogestionados StackSets

Cuenta	Finalidad	Acción en us-east-1	Acción en el us-west-2
111111111111	Administrador	Elimine la pila de funciones StackSet de administrador	Ninguno
222222222222	Miembro	Elimine la pila StackSet de funciones de ejecución	Ninguno

Guía para desarrolladores

En esta sección se proporciona el código fuente de la solución y personalizaciones adicionales.

Código fuente

Visite nuestro GitHub repositorio para descargar las plantillas y los scripts de esta solución y compartir sus personalizaciones con otras personas.

Libros de jugadas

Esta solución incluye las correcciones básicas para los estándares de seguridad definidos como parte del Centro de Seguridad de Internet (CIS) AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0,CIS AWS Foundations Benchmarkv3.0.0, AWS Foundational Security Best Practices (FSBP) v.1.0.0, Payment Card Industry Data Security Standard (PCI-DSS)v3.2.1 y National Institute of Standards and Technology (NIST).

Si tiene habilitadas las conclusiones de control consolidadas, todos los estándares admiten esos controles. Si esta función está habilitada, solo es necesario implementar el manual de estrategias de SC. De lo contrario, los manuales son compatibles con los estándares enumerados anteriormente.

> **Important**
>
> Utilice únicamente los manuales de estrategias para los estándares habilitados para evitar alcanzar las cuotas de servicio.

Para obtener más información sobre una solución específica, consulte el documento de automatización de Systems Manager con el nombre implementado por la solución en su cuenta. Vaya a la consola de AWS Systems Manager y, en el panel de navegación, seleccione Documentos.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
Remediaciones totales	63	34	29	33	65	19	90
ASR-EnableAutoScalingGroup ELBHealthCheck Los grupos de Auto Scaling asociados a un balanceador de cargas deben usar comprobaciones de estado del balanceador de cargas	Escalado automático.1		Escalado auto.1		Escalado auto.1		Escalado auto.1

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-ConfigureAutoScalingLaunchConfigToRequireIMDSv2 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 instancia					Escalado automático. 3		Escalado automático. 3

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
s (IMDSv2)							
ASR-CreateCloudTrailMultiRegionTrail CloudTrail debe activarse y configurarse con al menos un rastro multirregional	CloudTrail1.	2.1	CloudTrail2.	3.1	CloudTrail1.	3.1	CloudTrail1.
ASR-EnableEncryption CloudTrail debería tener activado el cifrado en reposo	CloudTrail2.	2.7	CloudTrail1.	3.7	CloudTrail2.	3.5	CloudTrail2.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableLogFileValidation Asegúrese de que la validación del archivo de CloudTrail registro esté activada	CloudTrail4.	2.2	CloudTrail3.	3.2	CloudTrail4.		CloudTrail4.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableCloudTrailToCloudWatchLogging Asegúrese de que las CloudTrail rutas estén integradas con Amazon CloudWatch Logs	CloudTrail5.	2.4	CloudTrail4.	3.4	CloudTrail5.		CloudTrail5.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR configura 3 BucketLogging Asegúrese de que el registro de acceso al bucket de S3 esté habilitado o en el bucket de S3 CloudTrail		2.6		3.6		3.4	CloudTrail7.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
SAR-ReplaceCodeBuildClearTextCredentials CodeBuild Las variables de entorno del proyecto no deben contener credenciales de texto claro	CodeBuild 2.		CodeBuild 2.		CodeBuild 2.		CodeBuild 2.
Habilitar ASR AWSConfig Asegúrese de que AWS Config esté activado	Config.1	2,5	Config.1	3.5	Config.1	3.3	Config.1

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-Make Private EBSSnapshots Las instantáneas de Amazon EBS no deberían poder restaurarse públicamente	EC21.		EC21.		EC21.		EC21.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EliminarVPCDefaultSecurityGroupRules El grupo de seguridad predeterminado de VPC debe prohibir el tráfico entrante y saliente	EC22.	4.3	EC22.	5.3	EC22.	5.4	EC22.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
Registros habilitados para ASR VPCFlow El registro de flujo de VPC debe estar habilitado en todos VPCs	EC26.	2.9	EC26.	3.9	EC26.	3.7	EC26.
SAR-EnableEbsEncryptionByDefault El cifrado predeterminado de EBS debe estar activado	EC27.	2.2.1			EC27.	2.2.1	EC27.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
SAR-RevokeUnrotatedKeys Las claves de acceso de los usuarios deben rotarse cada 90 días o menos	IAM.3	1.4		1.14	IAM.3	1.14	IAM.3
Política ASR IAMPassword Política de contraseñas predeterminada de IAM	IAM.7	1.5-1.11	IAM.8	1.8	IAM.7	1.8	IAM.7

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
Credenciales ASR-RevokeUnusedIAMUser Las credenciales de usuario deben desactivarse si no se utilizan en un plazo de 90 días	IAM.8	1.3	IAM.7		IAM.8		IAM.8

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-RevokeUnusedIAMUserCredentials Las credenciales de usuario deben desactivarse si no se utilizan en un plazo de 45 días				1.12		1.12	IAM.22
ASR-RemoveLambdaPublicAccess Las funciones Lambda deberían prohibir el acceso público	Lambda.1		Lambda.1		Lambda.1		Lambda.1

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-MakePrivateRDSSnapshot Las instantáneas de RDS deberían prohibir el acceso público	RDS.1		RDS.1		RDS.1		RDS.1
ASR-DisablePublicAccessToRDSInstance Las instancias de base de datos de RDS deberían prohibir el acceso público	RDS.2		RDS.2		RDS.2	2.3.3	RDS.2

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
Encriptar con ASR RDSSnapshot Las instantáneas del clúster de RDS y las instantáneas de las bases de datos deben cifrarse en reposo	RED.4				RED.4		RDS.4

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableMulti AZOnRDSInstance Las instancias de base de datos de RDS deben configurarse con varias zonas de disponibilidad	RDS.5				RDS.5		RDS.5

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableEnhancedMonitoringOnRDSInstance Se debe configurar una supervisión mejorada para las instancias y los clústeres de bases de datos de RDS	RDS.6				RDS.6		RDS.6

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
Habilitar ASR RDSCluster DeletionProtection Los clústeres de RDS deben tener activada la protección contra la eliminación	RDS.7				RDS.7		RDS.7

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
Habilitar ASR RDSInstance DeletionProtection Las instancias de base de datos de RDS deben tener activada la protección contra la eliminación	RDS.8				RDS.8		RDS.8

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableMinorVersionUpgradeOnRDSDBInstance Deben activarse las actualizaciones automáticas de las versiones secundarias de RDS	RDS.13				RDS.13	2.3.2	RDS.13

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableCopyTagsToSnapshotOnRDSCluster Los clústeres de bases de datos de RDS deben configurarse para copiar etiquetas en las instantáneas	RDS.16				RDS.16		RDS.16

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-DisablePublicAccessToRedshiftCluster Los clústeres de Amazon Redshift deberían prohibir el acceso público	Redshift.1		Redshift.1		Redshift.1		Redshift.1

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableAutomaticSnapshotsOnRedshiftCluster Los clústeres de Amazon Redshift deberían tener activadas las instantáneas automáticas	Redshift.3				Redshift.3		Redshift.3

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableRedshiftClusterAuditLogging Los clústeres de Amazon Redshift deberían tener activado el registro de auditoría	Redshift.4				Redshift.4		Redshift.4

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableAutomaticVersionUpgradeOnRedshiftCluster Amazon Redshift debería tener activadas las actualizaciones automáticas a las versiones principales	Redshift.6				Redshift.6		Redshift.6

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR configura 3 PublicAccessBlock La configuración de acceso público en bloque S3 debe estar activada	S3.1	2.3	S3.6	2.1.5.1	S3.1	2.1.4	S3.1

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR configura 3 BucketPublicAccessBlock Los buckets de S3 deberían prohibir el acceso de lectura público	S3.2		S3.2	2.1.5.2	S3.2		S3.2

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR configura 3 BucketPublicAccessBlock Los buckets de S3 deberían prohibir el acceso de escritura público		S3.3					S3.3
ASR- S3 EnableDefaultEncryption Los buckets S3 deben tener activado el cifrado del lado del servidor	S3.4		S3.4	2.1.1	S3.4		S3.4

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
SSLBucketPolítica establecida por ASR Los buckets de S3 deberían requerir solicitudes para usar SSL	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-S3 BlockDenylist Los permisos de Amazon S3 concedidos a otras cuentas de AWS en las políticas de bucket deben estar restringidos	S3.6				S3.6		S3.6

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
La configuración de acceso público por bloqueo de S3 debe activarse a nivel de bucket	S3.8				S3.8		S3.8
ASR configura 3 BucketPublicAccessBlock Asegúrese de que el bucket de S3 en el que se CloudTrail inicia sesión no sea de acceso público		2.3					CloudTrail6.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
SAR-CreateAccessLoggingBucket Asegúrese de que el registro de acceso al bucket S3 esté activado en el bucket CloudTrail S3		2.6					CloudTrail7.
SAR-EnableKeyRotation Asegúrese de que la rotación creada por el cliente CMKs esté activada		2.8	KMS.1	3.8	KMS.4	3.6	KMS.4

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-CreateLogMetricFilterAndAlarm Asegurar que haya un filtro de métricas de registro y alarma para las llamadas a la API no autorizadas		3.1		4.1			Cloudwatch.1

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-CreateLogMetricFilterAndAlarm Asegúrese de que existan un registro, un filtro de métricas y una alarma para el inicio de sesión en AWS Management Console sin MFA		3.2		4.2			Cloudwatch.2

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-CreateLogMetricFilterAndAlarm Asegúrese de que existan un filtro de métricas de registro y una alarma para su uso por parte del usuario «root»		3.3	CW.1	4.3			Cloudwatch.3

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-CreateLogMetricFilterAndAlarm Garantizar que haya un filtro de métricas de registro y una alarma para los cambios de política de IAM		3.4		4.4			Cloudwatch. 4

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-CreateLogMetricFilterAndAlarm Asegúrese de que existan un registro métrico, un filtro y una alarma para los cambios CloudTrail de configuración		3.5		4.5			Cloudwatch. 5

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-CreateLogMetricFilterAndAlarm Asegúrese de que existan un registro, un filtro de métricas y una alarma para los errores de autenticación de AWS Management Console		3.6		4.6			Cloudwatch. 6

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-CreateLogMetricFilterAndAlarm 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		3.7		4.7			Cloudwatch. 7

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-CreateLogMetricFilterAndAlarm Garantizar que haya un filtro de métricas de registro y una alarma para los cambios de política de bucket de S3		3.8		4.8			Cloudwatch. 8

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-CreateLogMetricFilterAndAlarm Asegúrese de que existan un registro, un filtro métrico y una alarma para los cambios de configuración de AWS Config.		3.9		4.9			Cloudwatch.9

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-CreateLogMetricFilterAndAlarm Garantizar que haya un filtro de métricas de registro y una alarma para los cambios de grupos de seguridad		3.10		4.10			Cloudwatch. 10

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-CreateLogMetricFilterAndAlarm 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)		3.11		4.11			Cloudwatch. 11

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-CreateLogMetricFilterAndAlarm Asegurar que haya un filtro de métricas de registro y alarma de registro para los cambios a las puertas de enlace de la red		3.12		4.12			Cloudwatch. 12

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-CreateLogMetricFilterAndAlarm Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en la tabla de enrutamiento		3.13		4.13			Cloudwatch. 13

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-CreateLogMetricFilterAndAlarm Garantizar que haya un filtro de métricas de registro y una alarma para los cambios en la VPC		3.14		4.14			Cloudwatch. 14

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
AWS-DisablePublicAccessForSecurityGroup Asegurar que ningún grupo de seguridad permita la entrada desde 0.0.0.0/0 al puerto 22		4.1	EC25.		EC21.3		EC2.13

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
AWS-DisablePublicAccessForSecurityGroup Asegurar que ningún grupo de seguridad permita la entrada desde 0.0.0.0/0 al puerto 3389		4.2			EC21.4		EC2.14
Configurar ASR SNSTopicForStack	CloudFormation1.				CloudFormation1.		CloudFormation1.
Crear rol de ASR IAMSupport		1.20		1,17		1,17	IAM.18

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-AsignarDisablePublicIPAuto EC2 Las subredes de Amazon no deberían asignar automáticamente direcciones IP públicas	EC21.5				EC2.15		EC2.15
SAR-EnableCloudTrailLogFileValidation	CloudTrail4.	2.2	CloudTrail3.	3.2			CloudTrail4.
ASR-EnableEncryptionFor SNSTopic	SNS.1				SNS.1		SNS.1

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableDeliveryStatusLoggingForSNSTopic El registro del estado de entrega debe estar habilitado para los mensajes de notificación enviados a un tema	SNS.2				SNS.2		SNS.2
ASR-EnableEncryptionFor SQSQueue	SQS.1				SQS.1		SQS.1

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
La instantánea RDS RDSSnapshot privada de ASR-Make debe ser privada	RDS.1		RDS.1				RDS.1
Bloqueo ASR SSMDocument PublicAccess Los documentos SSM no deben ser públicos	SSM 4				SSM.4		SSM.4

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableCloudFrontDefaultRootObject CloudFront las distribuciones deben tener un objeto raíz predeterminado configurado	CloudFront1.				CloudFront1.		CloudFront1.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-SetCloudFrontOriginDomain CloudFront las distribuciones no deben apuntar a orígenes S3 inexistentes	CloudFront.2				CloudFront.12		CloudFront.12

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
SAR-RemoveCodeBuildPrivilegedMode CodeBuild los entornos del proyecto deben tener una configuración de AWS de registro	CodeBuild 5.				CodeBuild 5.		CodeBuild 5.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
Instancia ASR-Terminate EC2 EC2 Las instancias detenidas deben eliminarse después de un período de tiempo específico	EC24.				EC24.		EC24.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
Habilitar ASR IMDSV2 OnInstance EC2 las instancias deben usar la versión 2 del servicio de metadatos de instancia () IMDSv2	EC28.				EC2.8.	5.6	EC2.8.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
SAR-RevokeUnauthorizedInboudRules Los grupos de seguridad solo deben permitir el tráfico entrante sin restricciones en los puertos autorizados	EC21.8				EC2.18		EC2.18

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
INSERTE AQUÍ EL TÍTULO Los grupos de seguridad no deben permitir el acceso irrestricto a los puertos de alto riesgo	EC2.19				EC2.19		EC2.19

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR desactivado TGWAutoAcceptSharedAttachments Amazon EC2 Transit Gateways no debería aceptar automáticamente las solicitudes de adjuntos de VPC	EC22.3				EC2.23		EC2.23

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
SAR-EnablePrivateRepositoryScanning Los repositorios privados de ECR deben tener configurado el escaneo de imágenes	ECR.1				ECR.1		ECR.1
ASR-EnableGuardDuty GuardDuty debería estar activado	GuardDuty 1.		GuardDuty 1.		GuardDuty 1.		GuardDuty 1.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR configura 3 BucketLogging Se debe habilitar el registro de acceso al servidor para un bucket de S3	S3.9				S3.9		S3.9

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableBucketEventNotifications Los buckets S3 deberían tener habilitadas las notificaciones de eventos	S3.11				S3.11		S3.11
ASR Sets 3 Lifecycle Policy Los buckets S3 deben tener configuradas las políticas de ciclo de vida	S3.13				S3.13		S3.13

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableAutoSecretRotation Los secretos de Secrets Manager deberían tener habilitada la rotación automática	SecretsManager1.				SecretsManager1.		SecretsManager1.
ASR-RemoveUnusedSecret Eliminación de secretos no utilizados de Secrets Manager	SecretsManager3.				SecretsManager3.		SecretsManager3.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-UpdateSecretRotationPeriod Los secretos de Secrets Manager deben rotarse en un número específico de días	SecretsManager4.				SecretsManager4.		SecretsManager4.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
Habilitar ASR APIGateway CacheData Encryption Los datos de la caché de la API de REST de API Gateway deben cifrarse en reposo					APIGateway5.		APIGateway5.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-SetLogGroupRetentionDays CloudWatch Los grupos de registros deben conservarse durante un período de tiempo específico					CloudWatch1.6		CloudWatch.16

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
SAR-AttachService VPCEndpoint Amazon EC2 debe configurarse para utilizar los puntos de enlace de VPC que se crean para el servicio de Amazon EC2	EC2.10				EC2.10		EC2.10

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
SAR-TagGuardDutyResource GuardDuty los filtros deben estar etiquetados							GuardDuty 2.
ASR-TagGuardDutyResource GuardDuty los detectores deben estar etiquetados							GuardDuty 4.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-Adjuntar SSMPermissions a EC2 EC2 Las instancias de Amazon deben ser gestionadas por Systems Manager	SSM.1		SSM.3				SSM.1

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-Configure LaunchConfigNoPublic IPDocument EC2 Las instancias de Amazon lanzadas mediante configuraciones de lanzamiento grupal de Auto Scaling no deben tener direcciones IP públicas					Autoscaling.5		Autoscaling.5
Habilitar ASR APIGateway Execution Logs	APIGateway1.						APIGateway1.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableMacie Amazon Macie debe estar habilitado	Macie.1				Macie.1		Macie.1
ASR-EnableAthenaWorkGroupLogging Los grupos de trabajo de Athena deben tener el registro habilitado	Athena.4						Athena.4

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-Enforce LAB HTTPSFor El Equilibrador de carga de aplicación debe configurarse para redirigir todas las solicitudes HTTP a HTTPS	ELB.1		ELB.1		ELB.1		ELB.1

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
Límite ASR ECSRootFilesystemAccess Los contenedores ECS deben estar limitados a un acceso de solo lectura a los sistemas de archivos raíz	ECS.5				ECS.5		ECS.5

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableElastiCacheBackups ElastiCache Los clústeres (Redis OSS) deben tener habilitadas las copias de seguridad automáticas	ElastiCache1.				ElastiCache1.		ElastiCache1.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableElastiCacheVersionUpgrades ElastiCache los clústeres deben tener habilitadas las actualizaciones automáticas de las versiones secundarias	ElastiCache2.				ElastiCache2.		ElastiCache2.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR-EnableElastiCacheReplicationGroupFailover ElastiCache los grupos de replicación deben tener habilitada la conmutación por error automática	ElastiCache3.				ElastiCache3.		ElastiCache3.

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR: escalado Configure DynamoDBAuto Las tablas de DynamoDB deberían escalar automáticamente la capacidad en función de la demanda	DynamoDB.1				DynamoDB.1		DynamoDB.1
ASR: TagDynamoDBTable recurso Las tablas de DynamoDB deben estar etiquetadas							DynamoDB.5

Descripción	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de control de seguridad
ASR: EnableDynamoDBDeletionprotección Las tablas de DynamoDB deben tener la protección contra eliminación habilitada					DynamoDB.6		DynamoDB.6

Añadir nuevas soluciones

Las soluciones se pueden añadir manualmente actualizando los archivos del manual de estrategias correspondientes o mediante programación ampliando la solución mediante construcciones de CDK, según el flujo de trabajo que prefiera.

> **Note**
>
> Las instrucciones que figuran a continuación aprovechan los recursos instalados por la solución como punto de partida. Por convención, la mayoría de los nombres de los recursos de la solución contienen el ASR and/or SO0111 para facilitar su localización e identificación.

Descripción general del flujo de trabajo manual

Los runbooks de Automated Security Response en AWS deben seguir la siguiente denominación estándar:

ASR- *<standard>* - - *<version>* *<control>*

Estándar: abreviatura del estándar de seguridad. Debe coincidir con los estándares admitidos por ASR. Debe ser uno de los siguientes valores: «CIS», «AFSBP», «PCI», «NIST» o «SC».

Versión: la versión del estándar. De nuevo, debe coincidir con la versión compatible con ASR y con la versión de los datos de búsqueda.

Control: el ID de control del control que se va a corregir. Debe coincidir con los datos de búsqueda.

1. Cree un manual en la (s) cuenta (s) de los miembros.
2. Cree un rol de IAM en las cuentas de los miembros.
3. (Opcional) Cree una regla de corrección automática en la cuenta de administrador.

Paso 1. Crea un manual en la (s) cuenta (s) de los miembros

1. Inicie sesión en la consola de AWS Systems Manager y obtenga un ejemplo de cómo encontrar JSON.
2. Cree un manual de automatización que corrija el hallazgo. En la pestaña De mi propiedad, utilice cualquiera de los `ASR-` documentos de la pestaña Documentos como punto de partida.
3. Las AWS Step Functions de la cuenta de administrador ejecutarán su manual. El runbook debe especificar la función de corrección para poder pasarla al ejecutar el runbook.

Paso 2. Cree un rol de IAM en las cuentas de los miembros

1. Inicie sesión en la consola de AWS Identity and Access Management.
2. Obtenga un ejemplo de las funciones SO0111 de IAM y cree una nueva. El nombre del rol debe empezar por SO0111-Remediate- - -. *<standard>* *<version>* *<control>* Por ejemplo, si se agrega el control 5.6 de CIS v1.2.0, el rol debe ser. `SO0111-Remediate-CIS-1.2.0-5.6`
3. Con este ejemplo, cree una función con el ámbito adecuado que permita únicamente las llamadas a la API necesarias para realizar la corrección.

En este momento, su corrección está activa y disponible para su corrección automática desde la acción personalizada de ASR en AWS Security Hub.

Paso 3: (opcional) Cree una regla de corrección automática en la cuenta de administrador

La corrección automática (no «automatizada») es la ejecución inmediata de la corrección tan pronto como AWS Security Hub reciba el hallazgo. Considere detenidamente los riesgos antes de utilizar esta opción.

1. Consulte un ejemplo de regla para el mismo estándar de seguridad en CloudWatch Events. El estándar de nomenclatura de las reglas es`standard_control_*AutoTrigger*`.
2. Copie el patrón de eventos del ejemplo que se va a utilizar.
3. Cambia el `GeneratorId` valor para que coincida con el `GeneratorId` de tu JSON de Finding.
4. Guarda y activa la regla.

Descripción general del flujo de trabajo de CDK

En resumen, se modificarán o agregarán los siguientes archivos del repositorio de ASR. En este ejemplo, se agregó una nueva corrección para la versión ElastiCache .2 a los manuales de estrategias de SC y AFSBP.

> **Note**
>
> Todas las correcciones nuevas deben añadirse al manual de estrategias de la SC, ya que en él se consolidan todas las soluciones disponibles en el ASR. Si tiene la intención de implementar solo un conjunto específico de manuales (por ejemplo, AFSBP), puede: (1) añadir la corrección únicamente a los manuales de estrategias previstos o (2) añadir la corrección a todos los manuales para los que exista en el estándar de Security Hub correspondiente, además del manual de estrategias de SC. Se recomienda utilizar la segunda opción por motivos de flexibilidad.

En este ejemplo, ElastiCache .2 se incluye en los siguientes estándares de Security Hub:

- AFSBP
- 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

Como, de forma predeterminada, ASR solo implementa guías para AFSBP y NIST.800-53, añadiremos esta nueva corrección a esas guías además de a las de SC.

Modify

- source/lib/remediation-runbook-stack.ts
- source/playbooks/AFSBP/lib/[nombre estándar] _remediations.ts
- source/playbooks/NIST80053/lib/control_runbooks-construct.ts
- source/playbooks/NIST80053/lib/[nombre estándar] _remediations.ts
- source/playbooks/SC/lib/control_runbooks-construct.ts
- source/playbooks/SC/lib/sc_remediations.ts
- source/test/regex_registry.ts

Add

- source/playbooks/SC/ssmdocs/SC_ .2.ts ElastiCache
- source/playbooks/SC/ssmdocs/descriptions/ElastiCache.2.md
- source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml

> **Note**
>
> El nombre elegido para el runbook puede ser cualquier cadena, siempre que sea coherente con el resto de los cambios realizados.

- source/playbooks/NIST80053/ssmdocs/NIST80053_2.ts ElastiCache
- source/playbooks/AFSBP/ssmdocs/AFSBP_ ElastiCache .2.yaml

Pasos de desarrollo

1. Cree el manual de remediación.
2. Cree los manuales de control.
3. Integre cada manual de control con un manual de estrategias.
4. Cree la función de IAM de remediación e integre el manual de remediación
5. Actualice las pruebas unitarias

Paso 1: Crear el manual de remediación

Este es el documento SSM que se utiliza para corregir los recursos. Debe incluir el `AutomationAssumeRole` parámetro, que es la función de IAM con permisos para ejecutar la corrección. Vea el archivo existente `source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml` como referencia al crear nuevos manuales de corrección.

Todos los manuales de ejecución nuevos deben añadirse al directorio. `source/remediation_runbooks/`

Paso 2: Crear los manuales de control

Un manual de control es un manual específico de un manual de estrategias que analiza los datos de búsqueda de un estándar determinado y ejecuta el manual de remediación correspondiente. Como vamos a añadir la corrección ElastiCache .2 a los manuales SC, AFSBP y NIST8 0053, debemos crear un nuevo manual de control para cada una de ellas. Se crean los siguientes archivos:

- source/playbooks/SC/ssmdocs/SC_ ElastiCache .2.ts
- source/playbooks/NIST80053/ssmdocs/NIST80053_ .2.ts ElastiCache
- source/playbooks/AFSBP/ssmdocs/AFSBP_ ElastiCache .2.yaml

Example

<PLAYBOOK_NAME><CONTROL.ID>El nombre de estos archivos es importante y debe seguir el formato _ .ts/yaml

Algunos manuales de ASR admiten manuales de control de IaC TypeScript, mientras que otros deben escribirse en formato YAML sin procesar. Consulte las soluciones existentes en el manual de estrategias correspondiente como ejemplos. En este ejemplo, analizaremos el manual de estrategias del SC, que utiliza el IaC.

En el manual de estrategias de SC, el nuevo manual de control debe exportar una clase que se extienda ControlRunbookDocument y coincida con el nombre del manual de correcciones. Eche un vistazo al siguiente ejemplo:

```
export class EnableElastiCacheVersionUpgrades extends ControlRunbookDocument {
  constructor(scope: Construct, id: string, props: ControlRunbookProps) {
    super(scope, id, {
      ...props,
      securityControlId: 'ElastiCache.2',
      remediationName: 'EnableElastiCacheVersionUpgrades',
      scope: RemediationScope.REGIONAL,
      resourceIdRegex: <Regex>,
      resourceIdName: 'ClusterId',
      updateDescription: new StringFormat('Automatic minor version upgrades enabled for
 cluster %s.', [
        StringVariable.of(`ParseInput.ClusterId`),
      ]),
    });
  }
}
```

- `securityControlId`es el identificador de control de la corrección que va a agregar, tal como se define en la vista de controles consolidados de Security Hub.
- `remediationName`es el nombre que ha elegido para el manual de correcciones.
- `scope`es el ámbito del recurso que se va a corregir e indica si existe a nivel mundial o en una región específica.
- `resourceIdRegex`es la expresión regular que se utiliza para capturar el ID del recurso que desea pasar al manual de correcciones como parámetro. Solo se debe capturar un grupo, no se deben capturar todos los demás grupos. Si desea pasar todo el ARN, omita este campo.
- `resourceIdName`es el nombre que desea establecer para el identificador del recurso con el que se capturó; debe coincidir con `resourceIdRegex` el nombre del parámetro del identificador del recurso que figura en el manual de correcciones.
- `updateDescription`es la cadena que desea asignar a la sección de «notas» del hallazgo en Security Hub una vez que la corrección se haya realizado correctamente.

También debe exportar una función llamada `createControlRunbook` que devuelve una nueva instancia de su clase. En el ElastiCache caso de la versión .2, esto se ve así:

```
export function createControlRunbook(scope: Construct, id: string, props:
 PlaybookProps): ControlRunbookDocument {
  return new EnableElastiCacheVersionUpgrades(scope, id, { ...props, controlId:
 'ElastiCache.2' });
}
```

donde `controlId` está el ID de control tal como se define en el estándar de seguridad asociado al manual de estrategias con el que se opera.

Si el control Security Hub tiene parámetros que le gustaría pasar al manual de correcciones, puede pasarlos añadiendo anulaciones a los siguientes métodos: -`getExtraSteps`: define los valores predeterminados para cada parámetro implementado para el control en Security Hub

> **Note**
>
> Cada parámetro de Security Hub debe tener un valor predeterminado

- `getInputParamsStepOutput`: define los resultados del GetInputParams paso del manual de control
- Cada salida tiene un `nameoutputType`, `yselector`. `selector`Debe ser el mismo selector utilizado en la anulación del `getExtraSteps` método.
- `getRemediationParams`: define los parámetros pasados al manual de correcciones, extraídos de los resultados de los pasos. GetInputParams

Para ver un ejemplo, navegue hasta el archivo. `source/playbooks/SC/ssmdocs/SC_DynamoDB.1.ts`

Paso 3: Integre cada manual de control con un manual

Para cada manual de control creado en el paso anterior, ahora debe integrarlo con las definiciones de infraestructura del manual asociado. Siga los pasos que se indican a continuación para cada manual de control.

> **Important**
>
> Si creó el manual de control utilizando YAML sin procesar en lugar de IaC mecanografiado, pase a la siguiente sección.

En */<playbook_name>/*`control_runbooks-construct.ts` Importa tu archivo de manual de control recién creado, de la siguiente manera:

```
import * as elasticache_2 from '../ssmdocs/SC_ElastiCache.2';
```

A continuación, vaya a la matriz de

```
const controlRunbooksRecord: Record<string, any>
```

Y añade una nueva entrada que asigne el ID de control (específico del playbook) al `createControlRunbook` método que has creado:

```
'ElastiCache.2': elasticache_2.createControlRunbook,
```

Añada el identificador de control específico del playbook a la lista de soluciones que se muestra a continuación: *<playbook_name>*`\_remediations.ts`

```
{ control: 'ElastiCache.2', versionAdded: '2.3.0' },
```

El `versionAdded` campo debe ser la última versión de la solución. Si al añadir la corrección se infringe el límite de tamaño de la plantilla, aumente el`versionAdded`. Puede ajustar el número de soluciones incluidas en cada pila de miembros del manual de estrategias. `solution_env.sh`

Paso 4: Cree la función de IAM de remediación e integre el manual de remediación

Cada remediación tiene su propia función de IAM con los permisos personalizados necesarios para ejecutar el manual de remediación. Además, es necesario invocar el `RunbookFactory.createRemediationRunbook` método para añadir el manual de correcciones que creó en el paso 1 a las plantillas de la solución. CloudFormation

En el`remediation-runook-stack.ts`, cada remediación tiene su propio bloque de código en la clase. `RemediationRunbookStack` El siguiente bloque de código muestra la creación de una nueva función de IAM y la integración del manual de correcciones para la corrección de la versión .2: ElastiCache

```
    //-----------------------
    // EnableElastiCacheVersionUpgrades
    //
```

```
    {
      const remediationName = 'EnableElastiCacheVersionUpgrades'; // should match the
 name of your remediation runbook
      const inlinePolicy = new Policy(props.roleStack, `ASR-Remediation-Policy-
${remediationName}`);

      const remediationPolicy = new PolicyStatement();
      remediationPolicy.addActions('elasticache:ModifyCacheCluster');
      remediationPolicy.effect = Effect.ALLOW;
      remediationPolicy.addResources(`arn:${this.partition}:elasticache:*:
${this.account}:cluster:*`);
      inlinePolicy.addStatements(remediationPolicy);

      new SsmRole(props.roleStack, 'RemediationRole ' + remediationName, { // creates
 the remediation IAM role
        solutionId: props.solutionId,
        ssmDocName: remediationName,
        remediationPolicy: inlinePolicy,
        remediationRoleName: `${remediationRoleNameBase}${remediationName}`,
      });

      RunbookFactory.createRemediationRunbook(this, 'ASR ' + remediationName, { // adds
 the remediation runbook to the solution's cloudformation templates
        ssmDocName: remediationName,
        ssmDocPath: ssmdocs,
        ssmDocFileName: `${remediationName}.yaml`,
        scriptPath: `${ssmdocs}/scripts`,
        solutionVersion: props.solutionVersion,
        solutionDistBucket: props.solutionDistBucket,
        solutionId: props.solutionId,
        namespace: namespace,
      });
    }
```

Paso 5: Actualizar las pruebas unitarias

Recomendamos actualizar y ejecutar las pruebas unitarias después de añadir una nueva solución.

En primer lugar, debe agregar cualquier expresión regular nueva (que aún no se haya agregado) al `source/test/regex_registry.ts` archivo. Este archivo exige pruebas para cada nueva expresión regular incluida en los manuales de ejecución de la solución. Eche un vistazo a la `addElastiCacheClusterTestCases` función como ejemplo, que se utiliza para probar las expresiones regulares utilizadas en ElastiCache las correcciones.

Por último, tendrás que actualizar las instantáneas de cada pila. Las instantáneas son definiciones de CloudFormation plantillas controladas por versiones que se utilizan para realizar un seguimiento de los cambios realizados en la infraestructura de ASR. Puede actualizar estos archivos de instantáneas ejecutando el siguiente comando desde el directorio: `deployment`

```
./run-unit-tests.sh update
```

¡Ahora está listo para implementar su nueva solución! Consulte la sección Compilar e implementar que aparece a continuación para obtener instrucciones sobre cómo crear e implementar la solución con los nuevos cambios.

Añadir un nuevo manual

Descargue los manuales de estrategias de soluciones de Automated Security Response on AWS y el código fuente de implementación del GitHub repositorio.

Los CloudFormation recursos de AWS se crean a partir de componentes del CDK de AWS y los recursos contienen el código de plantilla del manual de estrategias que puede utilizar para crear y configurar nuevos manuales de estrategias. Para obtener más información sobre cómo configurar su proyecto y personalizar sus manuales de estrategias, consulte el archivo README.md de. GitHub

Almacén de parámetros de AWS Systems Manager

Automated Security Response en AWS utiliza AWS Systems Manager Parameter Store para almacenar los datos operativos. Los siguientes parámetros se almacenan en el almacén de parámetros:

Nombre	Valor	Uso
`/Solutions/SO0111/CMK_REMEDIATION_ARN`	Clave de AWS KMS que cifrará los datos para las correcciones del FSBP	El cifrado de los datos de los clientes, como los CloudTrail registros, como parte de las correcciones
`/Solutions/SO0111/CMK_ARN`	Clave de AWS KMS que ASR utilizará para cifrar los datos	Cifrado de los datos de la solución

Nombre	Valor	Uso
`/Solutions/SO0111/SNS_Topic_ARN`	ARN del tema Amazon SNS para la solución	Notificación de eventos de corrección
`/Solutions/SO0111/SNS_Topic_Config.1`	Tema de SNS para las actualizaciones de AWS Config	Corrección de la configuración 1
`/Solutions/SO0111/sendAnonymousMetrics`	`Yes`	Recopilación de métricas anonimizadas
`/Solutions/SO0111/version`	Versión de la solución	
`/Solutions/SO0111/`*`<security standard long name>`*`/`*`<version>`* /status	`enabled`	Indica si el estándar está activo en la solución. Se puede deshabilitar un estándar para su corrección automática cambiándolo a `disabled`
`/Solutions/SO0111` // nombre corto *`<security standard long name>`*	`String`	Nombre abreviado del estándar de seguridad. Por ejemplo:`CIS`,`AFSBP`, `PCI`
`/Solutions/SO0111//`*`<security standard long name><version>`* /*`<control>`* /remap	`String`	Cuando un control usa la misma corrección que otro, estos parámetros realizan la reasignación

Tema de Amazon SNS: Progreso de la remediación

La respuesta de seguridad automatizada en AWS crea un tema de Amazon SNS, SO0111-ASR_Topic. Este tema se utiliza para publicar actualizaciones sobre el progreso de las correcciones. A continuación se muestran las tres posibles notificaciones que se envían a este tema.

```
Remediation queued for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
Remediation failed for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
[.replaceable]`<control_ID>` remediation was successfully invoke via AWS Systems
 Manager in account [.replaceable]`<account_ID>`
```

Este es el mensaje de finalización. Indica que la corrección se completó sin errores; sin embargo, la prueba definitiva para que la remediación se realice correctamente es la validación and/or manual de AWS Config Check.

Filtrar una suscripción a un tema de SNS

Políticas de filtrado de suscripciones de Amazon SNS:

1. Navegue hasta el tema de suscripción de SNS.
2. En la política de filtros de suscripciones, selecciona «Editar».
3. Expanda la sección «Política de filtros de suscripciones» y active la opción «Política de filtros de suscripciones» para activar los filtros.
4. Seleccione el ámbito «Cuerpo del mensaje».
5. Añada su política al editor JSON.
6. Guarde los cambios.

Políticas de ejemplo:

Filtrar por cuenta

```
  {
```

```
"finding": {
"account": [
"111111111111",
"222222222222"
]
}
```

Filtrar errores

```
{
"severity": ["ERROR"]
}
```

Filtrar por controles

```
{
"finding": {
"standard_control": ["S3.9","S3.6"]
}
}
```

Tema de Amazon SNS: Alarmas CloudWatch

Esta solución crea un tema de Amazon SNS,. `SO0111-ASR_Alarm_Topic` Este tema se utiliza para publicar alertas de alarma.

Los detalles de cualquier alarma que entre en el estado de ALARMA se enviarán a este tema.

Inicie Runbook on Config Findings

Esta solución puede iniciar manuales de ejecución en función de los resultados personalizados de AWS Config. Para ello, necesitará:

1. Busque el nombre de la regla de AWS Config que desee corregir. Esto se puede encontrar en AWS Config o en el hallazgo que Security Hub genera para esta regla.
2. Vaya a AWS Systems Manager Parameter Store y seleccione Create Parameter.
3. El nombre de la regla debe ser `/Solutions/SO0111/` [.replaceable] `Rule name from Step 1`

4. El valor debe tener el siguiente formato:

```
{
"RunbookName":"Name of SSM runbook",
"RunbookRole": "Role that Orchestrator will assume"
}
```

1. RunbookName es un campo obligatorio y será el manual que se ejecutará cuando corrija esta regla de Config. RunbookRole es la función que asumirá el orquestador al ejecutar esta función. No es un campo obligatorio y, si se omite, el orquestador utilizará de forma predeterminada el rol de miembro de la cuenta.
2. Una vez establecido esto, puede corregir la regla de Config mediante la acción personalizada «Remediar con ASR» que se encuentra en el Security Hub.

Referencia

Esta sección incluye información sobre una función opcional para recopilar métricas únicas para esta solución, sugerencias a recursos relacionados y una lista de los creadores que han contribuido a esta solución.

Recopilación de datos anonimizados

Esta solución incluye una opción para enviar métricas operativas anonimizadas a AWS. Utilizamos estos datos para comprender mejor cómo utilizan los clientes esta solución, así como los servicios y productos relacionados. Cuando está habilitada, se recopila la siguiente información y se envía a AWS:

- ID de solución: el identificador de la solución de AWS
- ID único (UUID): identificador único generado aleatoriamente para cada implementación de respuesta y remediación de AWS Security Hub
- Marca de tiempo: marca de tiempo de recopilación de datos
- Datos de instancia: información sobre la implementación de esta pila
- Configuración de la solución: funciones activadas y parámetros establecidos durante el lanzamiento inicial
- Estado: estado de implementación (solución aprobada o fallida) o (corrección aprobada o fallida)
- Mensaje de error: el mensaje de error genérico del campo de estado
- Generator_id: información sobre las reglas de Security Hub
- Tipo: nombre y tipo de remediación
- ProductARN: la región en la que se despliega Security Hub
- finding_triggered_by: el tipo de corrección realizada (acción personalizada o desencadenante automático)

AWS es propietario de los datos recopilados a través de esta encuesta. La recopilación de datos está sujeta al Aviso de privacidad de AWS. Para excluirse de esta función, complete los siguientes pasos antes de lanzar la CloudFormation plantilla de AWS.

1. Descargue la CloudFormation plantilla de AWS en su disco duro local.
2. Abra la CloudFormation plantilla de AWS con un editor de texto.

3. Modifique la sección de mapeo de CloudFormation plantillas de AWS desde:

```
Mappings:
Solution:
Data:
SendAnonymizedUsageData: 'Yes'
```

a:

```
Mappings:
Solution:
Data:
SendAnonymizedUsageData: 'No'
```

4. Inicie sesión en la CloudFormation consola de AWS.
5. Elija Crear pila.
6. En la página Crear pila, en la sección Especificar plantilla, seleccione Cargar un archivo de plantilla.
7. En Cargar un archivo de plantilla, seleccione Elegir archivo y después seleccione la plantilla editada de su unidad local.
8. Seleccione Siguiente y siga los pasos de la sección Lanzar la pila en la sección Implementación automatizada de esta guía.

Recursos relacionados

- Respuesta y corrección automatizadas con AWS Security Hub
- Análisis comparativos de Amazon Web Services Foundations del CIS, versión 1.2.0
- Estándar de prácticas recomendadas de AWS Foundational Security
- Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS, Payment Card Industry Data Security Standard) versión 3.2
- Instituto Nacional de Estándares y Tecnología (NIST) SP 800-53 Rev. 5

Colaboradores

Las siguientes personas y organizaciones han colaborado en este documento:

- Mike O'Brien
- Nikhil Reddy
- Chandini Penmetsa
- Chaitanya Deolankar
- Max Granat
- Tim Mekari
- Aaron Schuetter
- Andrew Yankowsky
- Josh Moss
- Ryan Garay
- Thiemo Belmega
- Mykhailo Markhain

Revisiones

Fecha de publicación: agosto de 2020 (última actualización: enero de 2025)

Visita ChangeLog.md en nuestro GitHub repositorio para realizar un seguimiento de las mejoras y correcciones específicas de cada versión.

Avisos

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. Este documento: (a) tiene únicamente fines informativos, (b) representa las ofertas y prácticas de productos actuales de AWS, que están sujetas a cambios sin previo aviso, y (c) no crea ningún compromiso ni garantía por parte de AWS y sus filiales, proveedores o licenciantes. Los productos o servicios de AWS se proporcionan «tal cual» sin garantías, declaraciones ni condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS con sus clientes están reguladas por los acuerdos de AWS, y este documento no forma parte de ningún acuerdo entre AWS y sus clientes ni lo modifica.

Automated Security Response en AWS se licencia según los términos de la versión 2.0 de la licencia Apache, disponible en The Apache Software Foundation.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.