Guía del usuario de

Agente de seguridad de AWS

Agente de seguridad de AWS: Guía del usuario de

Table of Contents

Introducción

Descubra qué hace AWS Security Agent, cómo funciona y cómo se combinan sus recursos.

¿Qué es AWS Security Agent?

AWS Security Agent es un agente pionero que protege sus aplicaciones de forma proactiva durante todo el ciclo de vida del desarrollo. Realiza revisiones de seguridad automatizadas y adaptadas a los requisitos de su organización, crea modelos de amenazas para identificar cómo podrían atacarse sus aplicaciones y ofrece pruebas de penetración contextuales bajo demanda. Al validar continuamente la seguridad desde el diseño hasta la implementación, AWS Security Agent ayuda a prevenir las vulnerabilidades de forma temprana en todos sus entornos.

Los equipos de seguridad definen los requisitos de seguridad de la organización una vez en la consola de AWS: bibliotecas de autorización aprobadas, estándares de registro y políticas de acceso a los datos. AWS Security Agent aplica automáticamente estos requisitos de seguridad durante todo el desarrollo, evaluando los documentos de arquitectura y el código en función de sus estándares y proporcionando orientación específica cuando detecta infracciones. De este modo, se garantiza una aplicación coherente de la seguridad para las revisiones del diseño y el código en todos los equipos.

Para la validación de la implementación, AWS Security Agent transforma las pruebas de penetración de un obstáculo periódico en una capacidad bajo demanda. Los equipos de seguridad proporcionan las URL de destino, los detalles de autenticación, el código fuente y la documentación de la aplicación. AWS Security Agent desarrolla una comprensión profunda de las aplicaciones y ejecuta cadenas de ataque sofisticadas para descubrir y validar las vulnerabilidades, lo que permite a los equipos realizar pruebas siempre que sea necesario.

Capacidades clave

AWS Security Agent ofrece funciones de seguridad integrales que abarcan todo el ciclo de vida del desarrollo.

Revisión de seguridad del diseño

AWS Security Agent se centra en la seguridad al proporcionar comentarios de seguridad en tiempo real sobre los documentos de diseño y evaluar el cumplimiento de los requisitos de seguridad de la organización antes de escribir cualquier código. Los equipos de seguridad suben los documentos a través de la aplicación web y reciben orientación sobre las medidas correctivas para priorizar los

hallazgos, lo que agiliza las laboriosas revisiones manuales y las convierte en análisis específicos. Al integrar de forma proactiva sus estándares de seguridad en cada revisión de diseño, reduce las modificaciones arquitectónicas tardías y mantiene el ritmo de los múltiples equipos de desarrollo.

Modelado de amenazas

AWS Security Agent crea modelos de amenazas de sus aplicaciones para identificar cómo podrían ser atacadas. Proporcione documentos de diseño técnico (documentos de alcance) para definir en qué se centra el agente, el código fuente como contexto para que el agente comprenda su sistema actual, o ambos. AWS Security Agent genera una descripción general del sistema que describe la arquitectura, los componentes, los límites de confianza, los flujos de datos y la postura de seguridad de su aplicación, junto con un conjunto de amenazas clasificadas por categoría de STRIDE (suplantación, manipulación, repudio, divulgación de información, denegación de servicio, elevación de privilegios) con niveles de gravedad y recomendaciones prácticas. Los modelos de amenazas son configuraciones reutilizables que puede volver a ejecutar a medida que el código y el diseño evolucionan, lo que permite realizar evaluaciones de seguridad iterativas a lo largo del ciclo de vida del desarrollo.

Revisión de la seguridad del código

AWS Security Agent protege las aplicaciones de forma proactiva mediante dos enfoques complementarios. En primer lugar, puede crear revisiones de código en la aplicación web para realizar escaneos exhaustivos de todo el código fuente desde GitHub los repositorios de Bitbucket o GitHub Enterprise Server o desde buckets S3, a fin de identificar las vulnerabilidades de seguridad y validar el cumplimiento de los requisitos organizativos en toda su base de código. GitLab En segundo lugar, puede habilitar el análisis automatizado de solicitudes de extracción para los repositorios conectados, donde AWS Security Agent revisa los cambios de código y publica los hallazgos de seguridad directamente como comentarios de solicitudes de extracción o solicitud de fusión. En ambos casos, los desarrolladores reciben una guía de corrección y AWS Security Agent puede generar automáticamente solicitudes de cambios o fusionar solicitudes con correcciones de código para las vulnerabilidades identificadas. Esto incorpora conocimientos de seguridad en todos los repositorios, lo que reduce las demoras relacionadas con la seguridad en el proceso de desarrollo y amplía la evaluación a todas las bases de código.

Pruebas de penetración

AWS Security Agent ofrece pruebas de penetración bajo demanda mediante el despliegue de agentes de IA especializados para descubrir, validar, informar y corregir las vulnerabilidades de

seguridad mediante escenarios de ataque personalizados de varios pasos. El agente entiende el contexto de la aplicación mediante el análisis del código fuente y la documentación para identificar y aprovechar las vulnerabilidades que las herramientas automatizadas de análisis de seguridad no pueden encontrar. Documenta los resultados mediante el análisis del impacto y las rutas de ataque reproducibles, y crea solicitudes de extracción con correcciones de código listas para su implementación, lo que transforma las evaluaciones periódicas en una validación continua que se extiende a todas las aplicaciones en lugar de limitarse solo a las más importantes.

Ventajas

On-demand accesibilidad

AWS Security Agent proporciona acceso inmediato a expertos en seguridad. Los equipos de desarrollo pueden realizar revisiones de diseño, modelos de amenazas, análisis de código y pruebas de penetración a pedido siempre que sea necesario, para adaptarse al ritmo de los ciclos de desarrollo modernos y permitir una seguridad proactiva en cada etapa.

Valide automáticamente los requisitos organizativos

Defina los requisitos de seguridad de su organización una vez en la consola de AWS. AWS Security Agent valida automáticamente estos requisitos en todas las aplicaciones durante cada revisión de diseño y seguridad del código, lo que garantiza que los equipos aborden sus requisitos específicos y no las listas de verificación genéricas.

Amplíe su experiencia en seguridad

AWS Security Agent escala las revisiones de seguridad para que coincidan con la velocidad de desarrollo mediante la automatización del cumplimiento de los requisitos de seguridad de la organización. Configure los requisitos de forma centralizada, lleve a cabo revisiones exhaustivas con análisis de los resultados y gestione los alcances de las pruebas de penetración en toda la organización a través de la consola de AWS.

Correcciones prácticas para vulnerabilidades confirmadas

AWS Security Agent valida los hallazgos de seguridad detectados durante las pruebas de penetración mediante una explotación basada en pruebas, ofrece rutas de exploits reproducibles y un análisis exhaustivo del impacto, y crea solicitudes de cambios con correcciones listas para su implementación en un lenguaje fácil de usar para los desarrolladores. Esto ayuda a los equipos

a centrarse en los riesgos de seguridad legítimos de alto impacto sin perder tiempo con falsos positivos.

Soporte para nubes múltiples e híbridas

AWS Security Agent funciona en entornos AWS, locales, híbridos, multinube y SaaS, lo que garantiza una orientación y pruebas de seguridad coherentes, independientemente de la infraestructura o plataforma que elija.

Capacidades de AWS Security Agent

AWS Security Agent ofrece cuatro funciones de seguridad principales a lo largo de su ciclo de vida de desarrollo:

- Revisión de la seguridad del diseño: revisa los documentos de diseño y arquitectura para identificar los riesgos de seguridad. Cargue los documentos a través de la aplicación web y el servicio los analizará en función de los requisitos de seguridad de su organización. AWS Security Agent evalúa el cumplimiento de sus requisitos de seguridad definidos, como las bibliotecas de autorización aprobadas, los estándares de registro y las políticas de acceso a los datos. Esto le ayuda a detectar diseños inseguros e infracciones de políticas al principio del proceso de desarrollo.
- Modelado de amenazas: crea un modelo de amenazas de su aplicación para identificar cómo podría ser atacada. Proporcione los documentos de diseño como documentos de alcance para definir el enfoque del análisis, el código fuente como contexto para que el agente comprenda su sistema actual, o ambos. AWS Security Agent genera una descripción general del sistema que describe la arquitectura, los componentes, los límites de confianza, los flujos de datos y la postura de seguridad de la aplicación, junto con un conjunto de amenazas clasificadas por categoría de STRIDE (suplantación, manipulación, repudio, divulgación de información, denegación de servicio, elevación de privilegios) con niveles de gravedad y recomendaciones prácticas. Cada amenaza está vinculada a las pruebas del código fuente.
- Revisión de la seguridad del código: analiza el código de sus repositorios y fuentes de S3 para identificar las vulnerabilidades de seguridad y las infracciones de los requisitos de seguridad de la organización en todos los lenguajes, marcos y arquitecturas. Crea revisiones de código en la aplicación web para realizar escaneos exhaustivos de todo el código fuente o habilita los comentarios de las solicitudes de extracción para revisar automáticamente los cambios en el código. GitHub AWS Security Agent proporciona una guía de corrección específica y puede generar automáticamente solicitudes de cambios con correcciones de código para las

vulnerabilidades identificadas. Esto garantiza la aplicación coherente de sus políticas de seguridad en todos los equipos de desarrollo.

- On-demand pruebas de penetración: descubre, valida, informa y corrige las vulnerabilidades de seguridad en las API y aplicaciones web activas mediante escenarios de ataque personalizados de varios pasos. Configure el servicio para crear una prueba de detección mediante la aplicación web especificando el alcance de las pruebas, los detalles de autenticación y los recursos. AWS Security Agent desarrolla el contexto de la aplicación a partir del código fuente y la documentación proporcionados y ejecuta cadenas de ataque sofisticadas para identificar las vulnerabilidades explotables que el análisis estático y las herramientas convencionales pasan por alto. También proporciona correcciones de código listas para su implementación y crea solicitudes de extracción directamente en su repositorio de código, lo que le permite resolver las vulnerabilidades aún más rápido.

Cómo funciona AWS Security Agent

AWS Security Agent funciona a través de tres interfaces para proporcionar una seguridad proactiva de las aplicaciones durante todo el ciclo de vida del desarrollo. Las configuraciones de seguridad se administran en la consola de administración de AWS, las revisiones de seguridad se llevan a cabo en la aplicación web Security Agent y la corrección automática del código y la búsqueda de seguridad se realiza directamente en plataformas de repositorio de código, como GitHub.

Descripción general de

AWS Security Agent consta de tres componentes principales:

- Consola de administración de AWS: configure los espacios de agentes, defina los requisitos de seguridad, configure las pruebas de penetración, conecte los repositorios de código y administre el acceso de los usuarios
- Aplicación web Security Agent: realice revisiones de diseño, cree y ejecute modelos de amenazas, ejecute pruebas de penetración, cree y ejecute revisiones de código y revise los hallazgos de seguridad en los espacios de agente asignados
- Integración del repositorio de código: reciba revisiones de código automatizadas en las solicitudes de extracción y en las solicitudes de corrección de pruebas de penetración. Actualmente, AWS Security Agent admite la conexión a GitHub.

Trabaja con AWS Security Agent en una de estas tres funciones, que puede identificar por la interfaz que utiliza:

Rol	Dónde trabaja y qué hace
Administrador	Funciona en la consola de administración de AWS: configura los espacios de agentes, define los requisitos de seguridad, configura las capacidades y administra el acceso de los usuarios.
Servicio	Funciona en la aplicación web Security Agent: realiza revisiones de diseño, modelos de amenazas, pruebas de penetración y revisiones de código, y analiza los resultados resultantes.
Desarrollador	Trabaja en un IDE GitHub o en un IDE (como Kiro o Claude Code): recibe automáticamente los resultados de seguridad en las solicitudes de incorpora ción de datos y escanea el código sin salir del entorno de desarrollo.

Usamos estos nombres de rol en todas partes para indicar quién realiza cada tarea. Una sola persona puede desempeñar más de un rol.

Configuración de la consola

Los administradores configuran AWS Security Agent a través de la consola de administración de AWS.

Espacios de agentes: cuando crea su primer espacio de agente en la consola de administración de AWS, AWS Security Agent crea la aplicación web para su cuenta. Cada espacio de agente que cree representa una aplicación o un proyecto distinto que desea proteger. En la aplicación web, los usuarios seleccionan en qué espacio de agente van a trabajar al realizar las evaluaciones de seguridad.

Requisitos de seguridad: defina los requisitos de seguridad que AWS Security Agent evalúa durante las revisiones del diseño y el código, organizados en paquetes de requisitos de seguridad. Habilite los AWS-managed paquetes según los estándares del sector, cree paquetes personalizados para las políticas de su organización o genere requisitos cargando su documentación de seguridad. Los requisitos se aplican a todos los espacios de agentes.

Configuración de las pruebas de penetración: configure las capacidades de las pruebas de penetración para cada espacio de agentes de la siguiente manera:

- Verificación de los dominios de destino para las pruebas mediante la verificación de DNS o HTTP
- Configuración del acceso a la VPC para probar aplicaciones privadas
- Configuración del CloudWatch registro para las ejecuciones de pruebas de penetración
- Configuración de las funciones de AWS Secrets Manager o Lambda para las credenciales de prueba
- Especificar buckets de S3 para un contexto de aplicación adicional

Configuración de revisión de código: configure las capacidades de revisión de código para cada espacio de agente de la siguiente manera:

- Conectar GitHub repositorios o depósitos de S3 que contienen código fuente
- Seleccionar la configuración de revisión del código (vulnerabilidades de seguridad, requisitos personalizados o ambos)
- Habilitar los comentarios mediante solicitudes de extracción para la revisión automática de los cambios de código en GitHub
- Configurar el CloudWatch registro para la revisión del código se ejecuta

Configuración del modelado de amenazas: configure las capacidades de modelado de amenazas para cada espacio de agente de la siguiente manera:

- Conectar repositorios de código fuente o depósitos S3 que contienen código fuente
- Añadir documentos de alcance (documentos de diseño de funciones) para centrar el análisis en una función específica
- Configurar el CloudWatch registro para las ejecuciones del modelo de amenazas
- Configuración de un rol de servicio para el acceso a los recursos de AWS

Integraciones: conecte GitHub los repositorios a cada espacio de agente para habilitar las capacidades clave:

- Proporcione el contexto de la aplicación para realizar pruebas de penetración más precisas
- Habilite la revisión del código para digitalizar todos los repositorios y analizar las solicitudes de extracción
- Habilite la corrección automática del código mediante solicitudes de extracción de datos para revisar el código y encontrar los resultados de las pruebas de penetración

Acceso de los usuarios: administre la forma en que los usuarios acceden a la aplicación web Security Agent. Si ha activado el Centro de identidad de IAM (SSO), asigne usuarios en la consola de AWS Security Agent para proporcionar acceso SSO directo a la aplicación web. Si utiliza el IAM-only acceso, los usuarios con acceso a la consola de AWS pueden lanzar la aplicación web a través del enlace de acceso de administrador de la consola para cualquier espacio de agente.

Actividades de aplicaciones web

Los usuarios acceden a la aplicación web Security Agent para realizar evaluaciones de seguridad en los espacios de agente asignados.

Seleccione el espacio de agente: al iniciar sesión en la aplicación web, los usuarios seleccionan en qué espacio de agente quieren trabajar. Los usuarios solo pueden ver y acceder a los espacios de agente a los que estén asignados.

Revisiones de diseño: cargue documentos de diseño y especificaciones de arquitectura para analizarlos en función de los requisitos de seguridad de la organización. Revise los hallazgos con una guía de remediación.

Modelos de amenazas: cree y ejecute modelos de amenazas proporcionando el código fuente, documentos de diseño técnico (documentos de alcance) o ambos. Los documentos de alcance definen en qué centra el agente su análisis; el código fuente proporciona un contexto sobre el sistema actual. Cada ejecución produce una descripción general del sistema que describe la arquitectura de la aplicación, los límites de confianza, los flujos de datos y la postura de seguridad, junto con un conjunto de amenazas clasificadas por categoría de STRIDE con niveles de gravedad y recomendaciones prácticas.

Revisiones de código: crea y ejecuta revisiones de código que realicen un análisis estático exhaustivo de todo el código fuente. Seleccione GitHub repositorios o fuentes de S3, configure los ajustes de escaneo y revise los hallazgos de seguridad detallados con una guía de corrección. AWS Security Agent identifica las vulnerabilidades de seguridad y valida el cumplimiento de los requisitos de seguridad personalizados de su organización en toda su base de código.

Pruebas de penetración: configure y ejecute las pruebas de penetración proporcionando las URL de destino, los detalles de autenticación y la documentación. AWS Security Agent realiza pruebas autónomas para descubrir vulnerabilidades explotables mediante escenarios de ataque de varios pasos.

Revise las conclusiones: analice detalladamente las conclusiones de seguridad extraídas de las revisiones de diseño, los modelos de amenazas, las revisiones del código y las pruebas de

penetración, incluidos los análisis de impacto, las rutas de ataque reproducibles y las directrices de remediación.

Valide las correcciones: evaluaciones Re-run de seguridad después de implementar las soluciones para verificar que se hayan abordado las vulnerabilidades.

GitHub integración

AWS Security Agent se integra directamente GitHub para proporcionar comentarios de seguridad automatizados en los flujos de trabajo de los desarrolladores.

Comentarios sobre las solicitudes de extracción: después de que los administradores instalen la GitHub aplicación AWS Security Agent y habiliten la revisión del código con comentarios de revisión del código para un espacio de agentes, AWS Security Agent analiza automáticamente las solicitudes de extracción en los repositorios conectados. Los desarrolladores reciben directamente en los comentarios de las solicitudes de extracción los datos de seguridad y las directrices sobre medidas correctivas. De este modo, se validan los cambios en el código en función de los requisitos de seguridad de la organización y de las vulnerabilidades más comunes.

Corrección automática: cuando los usuarios habilitan la corrección automática del código para una revisión del código, AWS Security Agent genera correcciones para las vulnerabilidades identificadas y envía solicitudes de extracción a los repositorios asociados. GitHub

Solución de las pruebas de penetración: cuando los administradores permiten buscar soluciones en la consola, los usuarios pueden solicitar la corrección automática de los hallazgos de las pruebas de penetración desde la aplicación web. AWS Security Agent abre una solicitud de cambios en el GitHub repositorio asociado con correcciones de código para corregir la vulnerabilidad.

Comprenda la jerarquía y el ciclo de vida de los recursos

AWS Security Agent organiza los recursos de pruebas de seguridad en una estructura jerárquica que determina lo que se comparte en la organización y el ámbito de aplicación. Comprender esta estructura le ayuda a configurar AWS Security Agent de forma eficaz y a saber dónde encontrar y gestionar los distintos recursos.

¿Qué se comparte en su organización

Algunos recursos de AWS Security Agent se configuran una vez a nivel organizativo y se aplican a todas sus aplicaciones y espacios de agentes. Estos recursos a nivel de inquilino proporcionan coherencia y reducen la duplicación del trabajo de configuración.

Recurso	Definición	¿Por qué se comparte
Requisitos de seguridad	Estándares de seguridad organizacional que definen lo que AWS Security Agent valida durante las revisiones del diseño y el código	Sus políticas de seguridad se aplican a todas las aplicaciones. Si los define una vez, AWS Security Agent los aplicará en todas partes.
GitHub integraciones	GitHub Organizaciones registradas o cuentas de usuario autorizadas para conectarse con AWS Security Agent	Registre su GitHub organización una vez y, a continuación, conecte repositorios específicos a cualquier espacio de agentes según sea necesario.
Configuraciones del IAM Identity Center	Configuración de SSO que controla la forma en que los usuarios acceden a AWS Security Agent	La administración centralizada de identidades se aplica a todos los espacios de agentes de su organización.

> **Important**
>
> Los cambios en los requisitos de seguridad afectarán a todas las futuras revisiones de diseño y de código en todos los Agent Spaces. Las revisiones existentes no se ven afectadas.

¿Cuál es el alcance de cada espacio de agente

Cada espacio de agente representa una aplicación o proyecto distinto que desea proteger. Los recursos a nivel de Agent Space se centran en esa aplicación específica, lo que permite a los diferentes equipos trabajar de forma independiente con sus propias configuraciones y evaluaciones.

Recurso	Definición	¿Por qué tiene un alcance por aplicación
Configuraciones de pruebas de penetración	Pruebe las configuraciones para funciones, puntos finales de API o	Cada aplicación tiene objetivos, métodos de autenticación y límites

Recurso	Definición	¿Por qué tiene un alcance por aplicación
	funciones específicas de su aplicació n	de alcance únicos específicos para esa aplicación.
Revisiones de diseño	Evaluaciones individuales de seguridad arquitectónica de los documentos de diseño	Cada aplicación tiene sus propios documentos de arquitectura y diseño que se evalúan de forma independi ente.
Modelos de amenazas	Evaluaciones de modelos de amenazas que ofrecen una visión general del sistema e identifican las amenazas a partir del código fuente, los documentos de diseño o ambos	Cada aplicación tiene su propio código y diseño, y las amenazas se modelan de forma independi ente. Los modelos de amenazas son configuraciones reutilizables que puede volver a ejecutar a medida que el código y el diseño evolucion an.
Integraciones	Proveedores de fuentes y documenta ción (Bitbucket GitHub GitLab, GitHub Enterprise Server y Confluence) conectados a este espacio de agentes	Las diferentes aplicaciones se basan en diferentes fuentes y documenta ción. Al conectarlas a nivel de Agent Space, se mantienen claros los límites de las aplicaciones.
Configuración de revisión de código	Configuración de las capacidades de revisión de código, incluidas las fuentes conectadas, la configura ción de escaneo y la activación de comentarios de relaciones públicas	Cada aplicación tiene sus propios repositorios y la revisión de seguridad debe configurarse de forma independiente.
Configuración de corrección de las pruebas de penetración	Configuración de los repositorios conectados que pueden recibir solicitudes de reparación automatiz adas para detectar los resultados de las pruebas de penetración	Los equipos controlan dónde AWS Security Agent puede enviar los cambios de código en función del flujo de trabajo de su aplicación.

Recurso	Definición	¿Por qué tiene un alcance por aplicación
Asignaciones de usuarios	Usuarios que tienen acceso a este espacio de agente específico	Los equipos solo ven las evaluaciones de seguridad de las aplicaciones de las que son responsables, lo que permite mantener el trabajo organizado y centrado.

> **Tip**
>
> Recomendamos crear un espacio de agentes por aplicación o proyecto para mantener límites claros entre los equipos y organizar las evaluaciones de seguridad de forma eficaz.

Cómo encajan GitHub los repositorios en la jerarquía

GitHub Los repositorios se integran mediante un proceso de varios pasos que conecta los recursos de la organización con aplicaciones específicas:

1. Regístrese a nivel de inquilino: autorice la GitHub aplicación AWS Security Agent para su GitHub organización o cuenta de usuario una vez
2. Conéctese a nivel de espacio de agente: seleccione repositorios específicos para conectarse a cada espacio de agente
3. Configure el uso por repositorio: habilite capacidades específicas para cada repositorio conectado:
   - Revisión del código: escaneo completo del código fuente y análisis automatizado de las solicitudes de extracción
   - Contexto de las pruebas de penetración: comprensión de la aplicación a partir del código fuente durante las pruebas de penetración
   - Corrección automática del código: solicitudes de extracción automatizadas con correcciones de vulnerabilidades para la revisión del código y los resultados de las pruebas de penetración

Se puede conectar un único repositorio a varios espacios de agentes con diferentes capacidades habilitadas en cada uno de ellos.

Diferencias clave entre las capacidades de seguridad

Cada capacidad de seguridad de AWS Security Agent sigue un modelo de flujo de trabajo diferente en función de cómo la utilizan los equipos de seguridad.

Pruebas de penetración: configuraciones reutilizables con ejecuciones independientes

Las pruebas de penetración utilizan un modelo de configuración y ejecución que admite las pruebas de seguridad iterativas:

- Cree una vez y ejecute varias veces: defina una configuración para un objetivo específico (punto final de la API, área de características) con los límites del alcance, la autenticación y los parámetros de prueba
- Ejecuciones independientes: ejecute la misma configuración varias veces para mejorar la seguridad. Cada ejecución es independiente y genera nuevos hallazgos

Este modelo admite la validación continua de la seguridad a medida que se desarrollan e implementan mejoras.

Revisiones de diseño: One-off evaluaciones con clonación

Las revisiones de diseño son evaluaciones independientes que no siguen un modelo de configuración reutilizable:

- Evaluación única: cada revisión de diseño analiza una vez los documentos cargados en función de los requisitos de seguridad de la organización
- No se puede volver a ejecutar: las revisiones de diseño no son reutilizables. No se puede volver a ejecutar la misma revisión
- Clonar para actualizarlo: clone una revisión de diseño existente para crear una nueva revisión con los documentos originales precargados, lo que le permitirá actualizar los documentos y ejecutar un nuevo análisis

Este modelo admite evaluaciones de seguridad arquitectónica puntuales.

Revisiones de código: configuraciones reutilizables con escaneos bajo demanda y análisis de relaciones públicas automáticos

Las revisiones de código ofrecen dos modos de operación para proteger el código fuente:

- Revisiones completas del código (aplicación web): cree configuraciones de revisión de código que seleccionen GitHub repositorios o fuentes de S3 y, a continuación, ejecute escaneos exhaustivos bajo demanda. Cada ejecución realiza un análisis estático de todo el código fuente y genera resultados con una guía de corrección. Puede volver a ejecutar la misma configuración de revisión de código a medida que el código evoluciona.
- Pull request comments (GitHub): habilita el análisis automatizado de los repositorios conectados GitHub . AWS Security Agent revisa automáticamente las solicitudes de cambios cuando están marcadas como listas para su revisión y publica directamente los hallazgos de seguridad en forma de comentarios GitHub.

Ambos modos utilizan los ajustes de revisión de código configurados (vulnerabilidades de seguridad, requisitos personalizados o ambos) y permiten la corrección automática del código mediante solicitudes de extracción.

Modelos de amenazas: configuraciones reutilizables con ejecuciones bajo demanda

Los modelos de amenazas utilizan un modelo de configuración y ejecución que permite la evaluación iterativa de la arquitectura:

- Cree una vez y ejecute varias veces: defina un modelo de amenazas seleccionando el código fuente como fuente, cargando los documentos de diseño como documentos de alcance o ambos. Ejecútelo cuando lo necesite y vuelva a ejecutarlo a medida que el código y el diseño evolucionen.
- Entradas flexibles: ejecute un modelo de amenazas solo en el código fuente, solo en los documentos de diseño o en ambos. Los documentos de alcance definen en qué centra el agente su análisis; el código fuente proporciona un contexto sobre el sistema actual.
- Descripción general del sistema y amenazas: cada ejecución produce una descripción general del sistema que describe la arquitectura de la aplicación, los límites de confianza, los flujos de datos y el nivel de seguridad de la aplicación, junto con un conjunto de amenazas clasificadas por categoría de STRIDE con su gravedad, pruebas y recomendaciones prácticas.

Comprender las relaciones entre los recursos

La jerarquía determina dónde se configuran los distintos recursos y se accede a ellos:

En la consola de administración de AWS:

- Configure los recursos a nivel de inquilino (requisitos de seguridad, GitHub integraciones, centro de identidad de IAM)
- Cree y gestione espacios de agentes
- Configure los ajustes de Agent Space (repositorios conectados, habilitación de la revisión del código, corrección de las pruebas de penetración)

En la aplicación web Security Agent:

- Cree y gestione las configuraciones de las pruebas de penetración y las ejecuciones de las pruebas
- Cree y gestione revisiones de diseño
- Cree, gestione y ejecute revisiones de código en repositorios conectados y fuentes de S3
- Cree, gestione y ejecute modelos de amenazas contra el código fuente, los documentos de alcance o ambos
- Vea los resultados de las pruebas de penetración, las revisiones de código, las revisiones de diseño y los modelos de amenazas

En GitHub:

- Vea los resultados de la revisión del código de las solicitudes de extracción como comentarios de las solicitudes de extracción
- Reciba solicitudes automatizadas de corrección para obtener información sobre la revisión del código y las pruebas de penetración (cuando estén habilitadas en el espacio de agentes)

> **Note**
>
> Los resultados de la revisión del código de las solicitudes de extracción aparecen en GitHub. Los resultados completos de la revisión del código, las pruebas de penetración y la revisión del diseño aparecen en la aplicación web Security Agent.

Introducción

Inscríbase, busque el punto de partida adecuado para su objetivo y ejecute su primera evaluación con un inicio rápido.

Inscríbase en un AWS inscrita

Para empezar AWS, necesitas una AWS cuenta. Para obtener información sobre cómo crear una AWS cuenta, consulta Cómo empezar con una AWS cuenta en la Guía de referencia de administración de AWS cuentas.

Selección de la ruta

Encuentre el punto de partida adecuado para lo que quiere hacer con AWS Security Agent. Utilice la siguiente tabla para hacer coincidir su objetivo con una tarea y, a continuación, vaya directamente a esa página. Si es la primera vez que utiliza AWS Security Agent, lea the section called "¿Qué es AWS Security Agent?" primero para obtener una breve descripción general.

Quiero...	¿Quién?	Empieza aquí
Comprenda lo que hace AWS Security Agent antes de configurarlo	A todos	the section called "¿Qué es AWS Security Agent?"
Configure el servicio y cree un espacio de agentes	Administrador	the section called "Configurar AWS Security Agent"
Pruebe mi aplicación activa o implementada para detectar vulnerabilidades explotables	Usuario	the section called "Inicio rápido: ejecutar una prueba de penetración"
Escanea mi código fuente para detectar vulnerabilidades e infracciones de las políticas	Usuario	the section called "Inicio rápido: ejecutar una revisión del código"
Modela cómo podrían atacar mi aplicación (STRIDE)	Usuario	the section called "Inicio rápido: Ejecute un modelo de amenazas"

Quiero...	¿Quién?	Empieza aquí
Obtenga comentarios de seguridad sobre un diseño antes de escribir el código	Usuario	the section called “Crear una revisión de diseño”
Escanea el código sin salir de mi IDE (Kiro o Claude Code)	Desarrollador	the section called “Ejecute escaneos de seguridad de código desde su IDE”
Escanea solo las líneas modificadas antes de fusionarlas	Desarrollador	the section called “Ejecute un escaneo de código diferencial con S3”
Recibe comentarios de seguridad automáticos sobre las solicitudes de extracción y fusión	Administrador	the section called “Habilitar la revisión de código”
Revisa los resultados y decide qué corregir primero	Usuario	Prueba de penetración, revisión del código, modelo de amenazas, revisión del diseño

> **Note**
>
> El agente de seguridad de AWS utiliza tres funciones, que puede identificar por la interfaz en la que trabaja: el administrador trabaja en la consola de administración de AWS (instalación y configuración), el usuario trabaja en la aplicación web (ejecuta las evaluaciones y revisa los resultados) y el desarrollador trabaja en GitHub un IDE como Kiro o Claude Code. Una sola persona puede desempeñar más de una función. Para ver las definiciones completas, consultethe section called “Cómo funciona AWS Security Agent”.

Inicio rápido: ejecutar una prueba de penetración

Esta guía de inicio rápido le guiará por la ejecución de su primera prueba de penetración (pentest) con AWS Security Agent. En una prueba de penetración, la aplicación implementada se compara con un dominio de destino verificado y arroja resultados de seguridad, cada uno con una clasificación de gravedad y pruebas que lo respalden. Abarca una aplicación de acceso público; para probar una alojada en una VPC privada, consulte. the section called “Habilitar la prueba de penetración”

> **Note**
>
> Necesita acceso a la consola de administración de AWS para configurar AWS Security Agent y definir el alcance de la prueba, y acceso a la aplicación web para crear y ejecutar pruebas de penetración.

Requisitos previos

Antes de empezar, asegúrese de que tiene lo siguiente:

- Acceso a la consola de administración de AWS con permisos para configurar AWS Security Agent.
- Un dominio de destino activo que aloja la aplicación que desea probar.
- La posibilidad de añadir un registro de DNS para ese dominio o una zona alojada de Route 53 en la misma cuenta de AWS, de forma que pueda verificar la propiedad.
- (Opcional) Un repositorio de código fuente (GitHub GitLab, o Bitbucket) para su aplicación, a fin de ofrecer más contexto al agente.

Paso 1: configurar el agente de seguridad de AWS en la consola de AWS

Si aún no ha configurado AWS Security Agent, complete la configuración inicial:

1. Navegue hasta AWS Security Agent en la consola de administración de AWS.
2. Seleccione Configurar AWS Security Agent.
3. Cree un espacio de agentes. Varios usuarios pueden usar un espacio de agente y debe ser específico para cada aplicación que desee probar. Introduzca un nombre y una descripción. El nombre debe identificar la aplicación que quieres probar de penetración.
4. Seleccione el IAM-only acceso en la configuración de acceso de usuario.
   - Esta guía de inicio rápido no incluye la activación del inicio de sesión único (SSO) con el IAM Identity Center, que permite a los usuarios acceder a la aplicación web directamente desde la consola de AWS.
   - Para permitir que los usuarios sin acceso a la consola de administración de AWS comiencen las pruebas de penetración, habilite la integración del centro de identidad de IAM. Para obtener más información, consulte the section called “Otorgue a los usuarios acceso a la aplicación web AWS Security Agent”.

5. Elija Configurar AWS Security Agent.

> **Note**
>
> Al elegir Configurar, AWS Security Agent crea su espacio de agente y establece una aplicación web en la que los usuarios pueden ejecutar pruebas de penetración, revisiones de código, modelos de amenazas y revisiones de diseño.

Paso 2: Habilite las pruebas de penetración y verifique su dominio

> **Note**
>
> En la consola de AWS, se define el alcance de lo que se puede probar. Luego, los usuarios ejecutan pruebas de penetración específicas dentro de ese ámbito desde la aplicación web.

1. En la barra lateral izquierda, selecciona Agent Spaces y, a continuación, selecciona el Agent Space que creaste en el paso 1.
2. Selecciona la pestaña Prueba de penetración y, a continuación, selecciona Configurar prueba de penetración para abrir el asistente.
3. Configurar el dominio: introduce el dominio de destino que quieres probar y selecciona un método de verificación, un registro TXT de DNS o una ruta HTTP. El dominio debe estar activo y alojar la aplicación que desea probar. Elija Siguiente.
4. Verificar dominios: compruebe la propiedad de cada dominio en la tabla de dominios de destino. AWS Security Agent solo realiza pruebas en dominios verificados. Para ver los pasos detallados y los valores exactos que se van a copiar, consultethe section called “Habilitar un dominio de aplicación para las pruebas de penetración”.
   - Route 53 dominios en la misma cuenta de AWS: seleccione el dominio y elija la One-click verificación. AWS Security Agent crea el registro de DNS y completa la verificación por usted.
   - Registro TXT de DNS (otros proveedores de DNS): en la tabla de dominios de destino, copie el nombre y el valor del registro, agréguelos como un registro TXT con su proveedor de DNS y, a continuación, seleccione el dominio y elija Verificar. Los cambios de DNS pueden tardar un tiempo en propagarse, por lo que es posible que la verificación no se complete de forma inmediata.

- Ruta HTTP: crea un archivo `.well-known/aws/securityagent-domain-verification.json` en tu servidor web, añade el token de verificación en el formato`{"tokens": ["<token>"]}`, selecciona el dominio y selecciona Verificar.

5. (Opcional) Configure capacidades adicionales: añada recursos opcionales, como grupos de CloudWatch registro y credenciales. La sección de acceso al servicio está preconfigurada: AWS Security Agent crea un rol de servicio con los permisos necesarios, a menos que elija un rol de IAM existente.

Paso 3: Conectar el código fuente (opcional)

La conexión con un proveedor de código fuente proporciona a AWS Security Agent un contexto sobre su aplicación y mejora la cobertura de las pruebas de penetración. Este paso es opcional.

1. En la pestaña Prueba de penetración, selecciona Añadir en el banner Conectar un proveedor de código fuente para las pruebas de penetración en la parte superior de la página.
2. Registre y conecte a su proveedor y, a continuación, seleccione los repositorios para ponerlos a disposición de los usuarios para las pruebas de penetración.

Para ver el flujo de integración completo, consulte Conectar AWS Security Agent a GitHub los repositorios o el tema de conexión de su proveedor.

Paso 4: Cree y ejecute una prueba de penetración

> **Note**
>
> Puede crear y ejecutar pruebas de penetración en la aplicación web AWS Security Agent. Recomendamos ejecutar las pruebas en un entorno de pruebas que refleje fielmente la producción.

1. Inicie la aplicación web: seleccione la pestaña Aplicación web y, a continuación, Acceso de administrador.
2. En la barra lateral izquierda, selecciona Pruebas de penetración y, a continuación, Crear una prueba de penetración.
3. Detalles de la prueba de penetración: configura el alcance de la prueba y la fuente del registro:
   a. Introduzca un nombre para Pentest.

b. En URL de destino, seleccione o introduzca un dominio verificado para probarlo (por ejemplo,`https://example.com`). Solo se pueden probar los dominios verificados y los subdominios se cubren automáticamente.

c. (Opcional) En URL accesibles, añade dominios a los que el agente debe acceder para iniciar sesión y navegar, pero que no debe atacar, como proveedores de identidad, CDN o API ajenos al dominio de destino. AWS Security Agent puede acceder a estos dominios, pero no los prueba; solo se atacan los dominios de destino.

d. Revise las reglas de configuración de la red para confirmar qué puntos de enlace pueden y qué no pueden recibir tráfico durante la prueba.

e. En Permisos, seleccione un rol de servicio y, si lo desea, un grupo de CloudWatch registros. Elija Siguiente.

4. (Opcional) Recursos de VPC: configura una VPC si tu objetivo está en una red privada a la que no se pueda acceder públicamente. Consulte the section called “Habilitar la prueba de penetración”.
5. Recursos de autenticación (opcionales): proporciona credenciales para que el agente pueda acceder a rutas autenticadas y no públicas. Recomendamos añadirlos para ampliar la cobertura y descubrir las vulnerabilidades que se esconden tras un inicio de sesión.
6. (Opcional) Configuración adicional: añada el contexto de la aplicación, como archivos, GitHub repositorios o fuentes de S3, para mejorar la calidad de las búsquedas. También puede activar la corrección automática del código y configurar otras opciones de ejecución aquí.
7. Seleccione Crear y ejecutar para iniciar la prueba ahora o Crear pentest para guardarla y ejecutarla más tarde.

Paso 5: Revise los resultados de las pruebas de penetración

1. Una prueba de penetración puede tardar varias horas en completarse. La mayoría se completa en 16 horas, según el tamaño y la complejidad de la solicitud.
2. La ejecución comienza con una fase de verificación previa que valida la configuración antes de que comiencen las pruebas: configura la infraestructura de registro, comprueba que se pueda acceder a los puntos finales de destino y prepara el entorno de pruebas. Si se produce un error en una comprobación previa (por ejemplo, si no se puede resolver un dominio de destino), la ejecución se detiene antes de que comiencen las pruebas. Abre la pestaña Preflight para ver qué comprobación ha fallado, resuélvela e inicia una nueva ejecución.
3. Cuando se complete la ejecución, ábrala y revise las pestañas Resumen de la ejecución, Registros y Resultados.

4. En la pestaña Hallazgos, seleccione un hallazgo para ver su descripción, gravedad, tipo de riesgo y pruebas que lo respalden.

Para obtener más información, consultathe section called “Crea una prueba de penetración” y the section called “Revise los resultados de una prueba de penetración”.

Inicio rápido: ejecutar una revisión del código

Esta guía de inicio rápido le guiará por la ejecución de su primera revisión de código con AWS Security Agent. AWS Security Agent escanea sus repositorios de código fuente para detectar vulnerabilidades de seguridad y cumplir con los requisitos de seguridad de su organización.

> **Note**
>
> Necesita acceso a la consola de administración de AWS para configurar AWS Security Agent y acceso a la aplicación web para crear y ejecutar revisiones de código.

Requisitos previos

Antes de empezar, asegúrese de que tiene lo siguiente:

- Acceso a la consola de administración de AWS con permisos para configurar AWS Security Agent.
- Un repositorio de código fuente (GitHub GitLab, o Bitbucket) o una fuente de Amazon S3 que contenga el código que quieres revisar.

Paso 1: Configurar AWS Security Agent en la consola de AWS

Si aún no ha configurado AWS Security Agent, complete la configuración inicial:

1. Navegue hasta AWS Security Agent en la consola de administración de AWS.
2. Seleccione Configurar AWS Security Agent.
3. Cree un espacio de agentes. Varios usuarios pueden usar un espacio de agente y debe ser específico para cada aplicación que desee probar. Introduzca un nombre y una descripción para su primer espacio de agentes. Este nombre aparece a los usuarios en la aplicación web. El nombre debe identificar la aplicación cuyo código desea revisar.
4. Seleccione el IAM-only acceso en la configuración de acceso de usuario.

- Esta guía de inicio rápido no incluye la activación del inicio de sesión único (SSO) con IAM Identity Center. Esto permite a los usuarios acceder directamente a la aplicación web AWS Security Agent desde la consola de AWS.
- Para permitir que los usuarios sin acceso a AWS Management Console accedan a las revisiones de código de ejecución, habilite la integración del IAM Identity Center. Para obtener más información, consulte the section called “Otorgue a los usuarios acceso a la aplicación web AWS Security Agent”.

5. Elija Configurar AWS Security Agent.

> **Note**
>
> Al elegir Configurar, AWS Security Agent crea su espacio de agente y establece una aplicación web en la que los usuarios pueden ejecutar pruebas de penetración, revisiones de código, modelos de amenazas y revisiones de diseño.

Paso 2: Habilitar y configurar la revisión del código

> **Note**
>
> Si ya tiene GitHub repositorios o depósitos de S3 conectados a su Agent Space (por ejemplo, mediante una configuración de pruebas de penetración), la revisión del código ya está habilitada. Puedes saltarte este paso e ir directamente a la aplicación web.

Abra el asistente de configuración de revisión de código

1. En la barra lateral izquierda, selecciona Agent Spaces y, a continuación, selecciona tu Agent Space.
2. Selecciona Habilitar la revisión de código en el encabezado o en la pestaña de revisión de código.

Connect integraciones, repositorios y depósitos

1. (Si aún no tienes una GitHub integración) Crea un registro. GitHub Si ya tienes uno, pasa al siguiente paso.

a. En la sección Integraciones conectadas, selecciona Añadir y, a continuación, Crear registro nuevo.

b. Seleccione GitHuby elija Siguiente.

c. Seleccione Instalar y autorizar y, a continuación, complete la instalación en GitHub:

   i. Seleccione el GitHub usuario o la organización propietario del repositorio que desea revisar.

   ii. Seleccione Todos los repositorios o Seleccione solo los repositorios.

   iii. Elija Instalar y autorizar y complete GitHub la autenticación.

d. De vuelta a la consola de administración de AWS, introduzca un nombre de registro y confirme que el tipo de cuenta coincide con el lugar donde instaló la GitHub aplicación.

e. Seleccione Connect para guardar el registro.

Para ver el flujo de GitHub integración completo, consulte Connect AWS Security Agent a los GitHub repositorios.

2. Connect GitHub repositorios. En la sección Integraciones conectadas, selecciona Añadir y, a continuación, selecciona tu GitHub registro. Se abre el GitHub asistente Connect de dos pasos:

   a. En Connect GitHub repositorios, seleccione los repositorios que desee incluir y pulse Siguiente.

   b. En Administrar las capacidades, alterne las siguientes opciones por repositorio:

      - Comentarios sobre la revisión del código: permita que AWS Security Agent publique los hallazgos de seguridad como comentarios en las solicitudes de cambios en el repositorio.
      - Solución automática: permita a los usuarios de la aplicación web AWS Security Agent solicitar solicitudes de cambios para corregir los hallazgos.

   c. Seleccione Guardar para volver al asistente de configuración.

3. (Opcional) Conecte las fuentes S3. En la sección de cubos de S3, selecciona Añadir recurso de S3 e introduce el URI de S3 de un depósito que contenga el código fuente, o selecciona Examinar para elegir uno.

4. Selecciona tu configuración de revisión de código. La opción predeterminada, Requisitos de seguridad y hallazgos de vulnerabilidades, analiza el código tanto para comprobar si cumple con los requisitos de seguridad que ha activado como para comprobar las vulnerabilidades más comunes.

5. Elija Siguiente.

Opciones de configuración opcionales

1. Configure los grupos de CloudWatch registros opcionales y el acceso a los servicios. El rol de servicio predeterminado está preconfigurado con los permisos necesarios.
2. Seleccione Save.

Paso 3: Crear y ejecutar una revisión de código

> **Note**
>
> Las revisiones de código se crean y ejecutan únicamente en la aplicación web AWS Security Agent.

1. Seleccione la pestaña Aplicación web y, a continuación, Acceso de administrador para lanzar la aplicación web AWS Security Agent.
2. En la barra lateral izquierda, selecciona Reseñas de código.
3. Selecciona Crear revisión de código.
4. Configura la revisión del código:
   a. Introduzca un título que identifique el alcance de esta revisión (por ejemplo, «billing-service-security-review»).
   b. En Fuentes, seleccione los GitHub repositorios que conectó a su espacio de agente en el paso 2 o introduzca las fuentes de S3 que desee analizar.
   c. Seleccione el rol de servicio de entre los roles configurados.
   d. (Opcional) Seleccione Habilitar la corrección automática de código para que AWS Security Agent envíe automáticamente solicitudes de cambios con correcciones para todos los hallazgos.
5. Elija Crear revisión de código.
6. En la página de detalles de la revisión del código, selecciona Iniciar revisión.

Paso 4: Revisa los resultados de la revisión del código

1. La revisión del código suele tardar entre 30 y 60 minutos, según el tamaño de la base de código.

2. La ejecución comienza con una fase de verificación previa que valida la configuración antes de que comience el escaneo: confirma que AWS Security Agent puede extraer el código fuente de su repositorio o fuente de S3 y configura el entorno de escaneo. Si se produce un error en una comprobación previa (por ejemplo, si no se puede acceder al código fuente), la ejecución se detiene antes del análisis estático. Abre la pestaña Preflight para ver qué comprobación ha fallado, resuélvela e inicia una nueva ejecución.
3. Una vez completada, navegue hasta la ejecución completada y seleccione la pestaña Hallazgos.
4. Revise los resultados en la vista de lista detallada:
   a. Seleccione un hallazgo en el panel izquierdo para ver sus detalles.
   b. Revisa las secciones Descripción, Ubicaciones del código, Pruebas y Soluciones sugeridas.
   c. Usa el código de remediación para generar una solicitud de cambios con una corrección, o revisa las relaciones públicas de remediación automática si has activado esa opción.

Para obtener más información, consultathe section called “Crear una revisión de código” y the section called “Revise los resultados de una revisión del código”.

Inicio rápido: Ejecute un modelo de amenazas

Esta guía de inicio rápido le mostrará cómo ejecutar su primer modelo de amenazas con AWS Security Agent. Un modelo de amenazas analiza la arquitectura de la aplicación y produce una descripción general del sistema (cómo AWS Security Agent entiende el sistema) y un conjunto de amenazas (cómo podría atacarse, cada una con un nivel de gravedad, una clasificación STRIDE y recomendaciones). Puede crear un modelo de amenazas a partir de documentos de diseño (documentos de alcance) para definir el enfoque, el código fuente (fuentes) para contextualizar su sistema actual, o ambos.

> **Note**
>
> Necesita acceso a la consola de administración de AWS para configurar AWS Security Agent y acceso a la aplicación web para crear y ejecutar modelos de amenazas.

Paso 1: Configurar AWS Security Agent en la consola de AWS

Si aún no ha configurado AWS Security Agent, complete la configuración inicial:

1. Navegue hasta AWS Security Agent en la consola de administración de AWS.
2. Seleccione Configurar AWS Security Agent.
3. Cree un espacio de agentes. Varios usuarios pueden usar un espacio de agente y debe ser específico para cada aplicación que desee proteger. Introduzca un nombre y una descripción para su primer espacio de agente. El nombre debe identificar la aplicación que quiere modelar como amenaza.
4. Seleccione el IAM-only acceso en la configuración de acceso de usuario.
   - Esta guía de inicio rápido no incluye la activación del inicio de sesión único (SSO) con IAM Identity Center. Esto permite a los usuarios acceder directamente a la aplicación web AWS Security Agent desde la consola de AWS.
   - Si desea permitir que los usuarios sin acceso a la consola de administración de AWS realicen tareas como iniciar un modelo de amenazas, debe habilitar la integración del centro de identidad de IAM.
5. Elija Configurar AWS Security Agent.

> **Note**
>
> Al elegir Configurar, AWS Security Agent crea su espacio de agente y establece una aplicación web en la que los usuarios pueden ejecutar pruebas de penetración, revisiones de código, modelos de amenazas y revisiones de diseño.

Paso 2: Conectar el código fuente

> **Note**
>
> Si ya tiene repositorios o depósitos de S3 conectados a su Agent Space (por ejemplo, mediante una revisión del código o una configuración de pruebas de penetración), puede omitir este paso e ir directamente a la aplicación web. Siempre puedes ejecutar un modelo de amenazas a partir de los documentos de alcance subidos sin necesidad de conectar ningún código fuente.

Connect repositorios o depósitos de S3 que contengan el código fuente que desee que el agente utilice como contexto para comprender su sistema actual:

1. En la barra lateral izquierda, selecciona Agent Spaces y, a continuación, selecciona tu Agent Space.
2. Ve a la sección Integraciones para conectar tu proveedor de código fuente.
3. Como alternativa, conecta los buckets de S3 que contengan tu código fuente.

Para ver el flujo de integración completo, consulte Connect AWS Security Agent a los GitHub repositorios.

Paso 3: Cree y ejecute un modelo de amenazas

> **Note**
>
> Los modelos de amenazas se crean y ejecutan en la aplicación web AWS Security Agent.

1. Inicie la aplicación web desde la pestaña de aplicaciones web de la consola de administración de AWS. Como alternativa, si ha configurado el Centro de identidades de IAM, inicie sesión directamente.
2. En la barra lateral izquierda, selecciona Modelos de amenazas.
3. Selecciona Crear modelo de amenazas.
4. Configure el modelo de amenazas:
   a. Introduzca un título que identifique el alcance de este modelo de amenaza (por ejemplo, «billing-service» o «checkout-api»).
   b. Proporcione al menos una entrada:
      - En los documentos de Scope, sube los documentos de diseño (DOC, DOCX, JPEG, MD, PDF, PNG o TXT), introduce los URI de S3 o selecciona las páginas de Confluence.
      - En Fuentes, selecciona los repositorios de las integraciones conectadas o introduce los URI de S3 que contengan el código fuente.

      > **Tip**
      >
      > Proporcione tanto las fuentes como los documentos de alcance para adaptar el modelo de amenazas a un diseño específico (por ejemplo, un documento de diseño de funciones) y, al mismo tiempo, proporcione al agente su código fuente como contexto para comprender su sistema actual.

c. Seleccione la función de servicio de entre las funciones configuradas.

d. (Opcional) Seleccione un grupo de CloudWatch registros para los registros.

5. Elija Crear modelo de amenazas.
6. En la página de detalles del modelo de amenazas, elija Iniciar ejecución.

Paso 4: Revise las amenazas

1. La ejecución avanza en sus tareas de análisis. Puede supervisar el progreso en la pestaña Preflight y ver los detalles de las tareas en la pestaña Registros.
2. Una vez completada, el estado de la ejecución cambia a Completada.
3. Seleccione la pestaña Descripción general para revisar la descripción general del sistema y la distribución de la gravedad.
4. Seleccione la pestaña Amenazas para revisar las amenazas identificadas:
   a. Seleccione una amenaza de la lista para ver sus detalles en el panel lateral.
   b. Revisa la declaración, la gravedad, las categorías de STRIDE, la recomendación, la evidencia y otros campos.
   c. Actualiza el estado de la amenaza a Resuelta o Descartada a medida que abordes o clasifiques cada amenaza.

Para obtener más información, consultathe section called “Cree un modelo de amenazas” y the section called “Revise las amenazas a partir de un modelo de amenazas”.

Para administradores (consola)

Como administrador, debe configurar AWS Security Agent en la consola de administración de AWS y configurar los Agent Spaces a los que acceden los usuarios a través de la aplicación web AWS Security Agent. Cada espacio de agente representa un entorno distinto con permisos y recursos específicos.

Recomendamos crear un espacio de agente único para cada aplicación que desee probar. Por ejemplo, si tiene dos proyectos internos (una aplicación de facturación y una aplicación de seguimiento de tareas), debe crear dos espacios de agentes independientes.

Configuración de ejemplo

Considere la posibilidad de que un administrador configure un espacio de agentes para evaluar la seguridad de una aplicación de facturación interna. El administrador haría lo siguiente:

- Verifica el dominio (por ejemplo`beta.billing.example.com`)
- Conéctese a GitHub y habilite la revisión de código
- Configure el acceso a la red asignando una VPC, una subred y un grupo de seguridad adecuados para las pruebas de penetración

Cuando los usuarios inician una prueba de penetración o una revisión del diseño, pueden seleccionar entre estos recursos preconfigurados y trabajar dentro de los límites que usted haya definido y, al mismo tiempo, mantener la flexibilidad para sus necesidades de evaluación específicas.

Configurar y crear espacios de agentes

Configure AWS Security Agent para su organización y cree los espacios de agentes que abarquen los recursos y las evaluaciones de cada aplicación.

Configurar AWS Security Agent

Configure AWS Security Agent para su organización creando su primer espacio de agente y estableciendo el modo en que los usuarios accederán a la aplicación web.

Esta configuración inicial permite a los administradores configurar las capacidades de seguridad en la consola de AWS y proporciona a los usuarios acceso a la revisión del diseño y a las pruebas de

penetración a través de la aplicación web Security Agent. Tras esta configuración única, puede crear espacios de agente adicionales con un proceso simplificado.

Descripción general de

Entendiendo los espacios de agentes

Un espacio de agentes es un espacio de trabajo dedicado para proteger una aplicación o un proyecto específicos. Contiene todas las revisiones de seguridad, los GitHub repositorios conectados opcionalmente, las configuraciones de las pruebas de penetración, los resultados y las conclusiones de esa aplicación.

Los Agent Spaces ayudan a organizar el trabajo de seguridad al mantener separadas las evaluaciones de seguridad de cada aplicación, lo que permite a los equipos centrarse en su aplicación específica. Recomendamos crear un Agent Space por aplicación o proyecto para mantener los límites claros.

Los requisitos de seguridad se definen a nivel de la organización y se aplican a todos los Agent Spaces, mientras que cada Agent Space mantiene sus propios documentos de diseño, repositorios de códigos, configuraciones de las pruebas de penetración, resultados de las pruebas de penetración y hallazgos de seguridad.

¿Qué incluye un espacio de agentes

Cada espacio de agente contiene:

- GitHub Repositorios conectados opcionalmente asociados a la aplicación o al proyecto
- Revisiones de diseño anteriores de la aplicación
- Configuraciones y límites de pruebas de penetración específicos de la aplicación
- Resultados de las pruebas de penetración y hallazgos de seguridad

Qué configurará durante la instalación

Durante esta primera configuración, tomará decisiones organizativas que se aplicarán a todos los espacios de agentes:

- Método de acceso: elija cómo accederán los usuarios a la aplicación web Security Agent (IAM Identity Center SSO o IAM-only accederán a través de la consola de AWS)
- Permisos: configure la función de IAM que utiliza la aplicación web para acceder a los servicios de AWS

- Primer espacio de agente: cree su espacio de agente inicial con un nombre y una descripción

> **Note**
>
> Tras completar esta configuración, crear espacios de agente adicionales es más sencillo: basta con indicar un nombre y una descripción. Consulte the section called “Crear un espacio de agentes” para obtener más información sobre la creación de espacios de agente posteriores.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Permisos para crear y administrar los recursos de AWS Security Agent
- Comprensión de los requisitos de administración de identidades de su organización
- (Opcional) Cuenta de AWS con permisos para crear funciones de IAM y configurar el centro de identidad de IAM (si se utiliza el acceso SSO)
- (Opcional) Función de IAM existente si desea utilizar una configuración de permisos personalizada

Paso 1: Crea tu primer espacio de agente

Defina las propiedades básicas de su primer espacio de agente que se mostrará a los usuarios en la aplicación web.

1. En la página de la consola de AWS Security Agent, elija Configurar Security Agent.
2. En el campo Nombre del espacio de agente, introduzca un nombre para su espacio de agente.

> **Note**
>
> El nombre del espacio de agente se muestra a los usuarios en la aplicación web y ayuda a identificar qué aplicación o proyecto representa este espacio.

3. (Opcional) En el campo Descripción, proporcione una descripción que ayude a distinguir el propósito del espacio de agentes.

> **Tip**
>
> La descripción ayuda a distinguir el propósito del espacio de agentes. Recomendamos describir la aplicación o el proyecto específicos que protegerá este Agent Space, por ejemplo, «aplicación web para el portal de clientes», «microservicios de procesamiento de pagos» o «plataforma de análisis interna».

Paso 2: Elige tu método de acceso

Seleccione cómo accederán los usuarios a la aplicación web Security Agent. Puede elegir entre habilitar el acceso SSO a través del Centro de identidades de IAM o proporcionar el acceso a través de la consola de AWS.

> **Note**
>
> Si elige el IAM-only acceso y más adelante quiere utilizar el Centro de identidades de IAM, tendrá que eliminar la configuración de AWS Security Agent y volver a completar el proceso de configuración.

1. En la sección Método de acceso, seleccione una de las siguientes opciones:
   - Centro de identidad de IAM (SSO): habilite el acceso SSO para su equipo a través del Centro de identidad de IAM. Esta opción se recomienda para los equipos que necesitan una administración de usuarios centralizada y desean que los usuarios accedan a la aplicación web directamente sin tener que pasar por la consola de AWS.
   - IAM-only acceso: proporcione acceso a través de un enlace de acceso de administrador en la consola de AWS. Esta opción es más sencilla de configurar y adecuada para los equipos que prefieren el acceso desde una consola o que no requieren capacidades de SSO.
2. Si seleccionó el Centro de identidad de IAM (SSO), continúe con el paso 2a que se indica a continuación.
3. Si ha seleccionado el IAM-only acceso, vaya al paso 3.

Paso 2a: Configurar el centro de identidad de IAM (solo para acceso SSO)

Complete estos pasos solo si seleccionó el Centro de identidad de IAM (SSO) como método de acceso.

1. En la sección Connect to IAM Identity Center, consulte la región de AWS.

> **Important**
>
> La aplicación debe estar configurada en la misma región en la que habilita el Centro de identidad de IAM. La región que se muestra es donde se creará su espacio de agente. El Centro de identidad de IAM debe estar habilitado en la misma región en la que creó su espacio de agente.

2. En la sección Centro de identidad de IAM, elija una de las siguientes opciones:
   - Seleccione Crear instancia de cuenta para crear una nueva instancia de cuenta de IAM Identity Center
   - Si ya existe una instancia de la organización en la misma región, AWS Security Agent se conectará automáticamente a ella.

> **Note**
>
> Después de conectar AWS Security Agent al IAM Identity Center, puede administrar el acceso asignando usuarios del IAM Identity Center a la aplicación.

3. Si va a conectar Active Directory o a un proveedor de identidad externo, consulte la alerta informativa.

> **Important**
>
> Si ya administra usuarios en Active Directory o en otra fuente de identidad y planea conectar esa fuente de identidad al Centro de identidades de IAM, cancele la configuración y vaya primero a la consola del Centro de identidades de IAM. Elija la fuente de identidad a la que quiere conectarse antes de configurar AWS Security Agent. Si cambia las fuentes de identidad más adelante, es posible que se eliminen las asignaciones de usuarios existentes.

Paso 3: Configurar los permisos (opcional)

Configure la función de IAM que la aplicación web de Security Agent utiliza para acceder a los servicios, las API y las cuentas de AWS.

1. Busque la sección Configuración de permisos (opcional).
2. Si la sección está contraída, elija la sección de configuración de permisos para ampliarla.
3. Seleccione una de las siguientes opciones:
   - Crear rol predeterminado: AWS Security Agent crea automáticamente un nuevo rol de IAM con los permisos necesarios para la aplicación web
   - Utilice otro rol: seleccione un rol de IAM existente entre las opciones disponibles
4. Revise la descripción del rol:

> **Note**
>
> Se creará un rol de IAM predeterminado para que su aplicación web acceda a otros servicios, API y cuentas de AWS. Al rol se le concederán los permisos necesarios para las operaciones de evaluación de la seguridad.

Paso 4: completar la configuración

Tras configurar todos los ajustes necesarios, complete la configuración para crear su primer espacio de agente y establecer la aplicación web Security Agent.

1. Revise todas las secciones de configuración para garantizar su precisión.
2. Elija Configurar.
3. AWS Security Agent crea su espacio de agente, establece la aplicación web y configura los recursos de AWS necesarios.

> **Note**
>
> Tras la configuración inicial, tendrá la opción de configurar las capacidades, incluidos los límites de las pruebas de penetración, los requisitos de seguridad y GitHub la integración.

Siguientes pasos

Tras configurar AWS Security Agent:

- Defina los requisitos de seguridad de su organización
- Configure las capacidades de pruebas de penetración, incluida la verificación del dominio y el acceso a la VPC, para su espacio de agente
- Connect GitHub repositorios para el contexto de revisión de código y pruebas de penetración
- (Si utiliza el Centro de identidad de IAM) Asigne usuarios al espacio de agentes de la consola de AWS Security Agent
- (Si utiliza el IAM-only acceso) Inicie la aplicación web a través del enlace de acceso de administrador de la consola de AWS
- Cree espacios de agentes adicionales para otras aplicaciones (consultethe section called “Crear un espacio de agentes”)

Crear un espacio de agentes

Cree espacios de agentes para proteger las aplicaciones o los proyectos de su organización. Cada espacio de agente proporciona un espacio de trabajo para realizar evaluaciones de seguridad, conclusiones y configuraciones específicas de esa aplicación o proyecto, y varios usuarios pueden acceder a él.

Este procedimiento supone que ya ha completado la configuración inicial del AWS Security Agent. Si aún no ha configurado AWS Security Agent, consultethe section called “Configurar AWS Security Agent”.

Descripción general de

Descripción de los espacios de agentes

Un espacio de agentes es un espacio de trabajo dedicado a proteger una aplicación o proyecto específico. Contiene todas las revisiones de seguridad, los repositorios de código conectados opcionalmente, las configuraciones de las pruebas de penetración, los resultados y las conclusiones de esa aplicación.

Los Agent Spaces ayudan a organizar el trabajo de seguridad al mantener separadas las evaluaciones de seguridad de cada aplicación, lo que permite a los equipos centrarse en su

aplicación específica. Recomendamos crear un Agent Space por aplicación o proyecto para mantener límites claros.

Para obtener una explicación completa de los Agent Spaces y de cómo se integran en la estructura de seguridad de su organización, consultethe section called “Comprenda la jerarquía y el ciclo de vida de los recursos”.

¿Qué incluye un espacio de agentes

Cada espacio de agente contiene:

- Repositorios de código conectados opcionalmente asociados a la aplicación o al proyecto
- Revisiones de diseño anteriores de la aplicación o el proyecto
- Pruebas de penetración: configuraciones y límites específicos de la aplicación
- Resultados de las pruebas de penetración y hallazgos de seguridad

Cree un espacio de agentes

Cree un nuevo espacio de agentes para una aplicación o un proyecto que desee proteger.

1. En la consola de AWS Security Agent, vaya a la página Agent Spaces.
2. Elija Crear espacio para agentes.
3. En el campo Nombre del espacio de agente, introduzca un nombre para su espacio de agente.

> **Note**
>
> El nombre del espacio de agente se muestra a los usuarios en la aplicación web y ayuda a identificar qué aplicación o proyecto representa este espacio.

4. (Opcional) En el campo Descripción, proporcione una descripción que ayude a distinguir el propósito del espacio de agentes.

> **Tip**
>
> La descripción ayuda a distinguir el propósito del espacio de agentes. Recomendamos describir la aplicación o el proyecto específicos que protegerá este Agent Space, por ejemplo, «aplicación web para el portal de clientes», «microservicios de procesamiento de pagos» o «plataforma de análisis interna».

5. Seleccione Crear.

> **Note**
>
> AWS Security Agent creará su espacio de agente. Ahora puede configurar las capacidades y conectar los recursos específicos de esta aplicación.

Siguientes pasos

Tras crear su espacio de agente:

- Connect repositorios de código fuente (GitHub GitLab, Bitbucket o GitHub Enterprise Server) para obtener un contexto de revisión de código y pruebas de penetración
- Connect Confluence para obtener el contexto de la documentación en las revisiones de diseño y las pruebas de penetración
- Habilite la función de revisión de código para los repositorios conectados (consulte) the section called “Habilitar la revisión del código de las solicitudes de extracción para los GitHub repositorios”
- Configure las capacidades de las pruebas de penetración, incluida la verificación del dominio
- (Si utiliza el Centro de identidad de IAM) Asigne usuarios a este espacio de agente en la sección de aplicaciones web de la página del espacio de agente. (consultethe section called “Otorgue a los usuarios acceso a la aplicación web AWS Security Agent”)
- (Si utilizan el IAM-only acceso) Los usuarios con acceso a la consola pueden iniciar la aplicación web a través del enlace de acceso de administrador de este espacio de agente

Connect integraciones

Conecte y gestione los proveedores de código fuente (GitHubBitbucket y GitHub Enterprise Server) y los proveedores de documentación (Confluence), junto con la conectividad de red privada, que sus Agent Spaces utilizan para la revisión del código, las pruebas de penetración y el modelado de amenazas. GitLab

Cómo funcionan las integraciones con Agent Spaces

AWS Security Agent se conecta con proveedores de documentación y código fuente de terceros para que el agente pueda analizar el código y la documentación durante las evaluaciones de

seguridad. Antes de contactar con un proveedor específico, es útil entender cómo se relacionan las integraciones con los espacios y las capacidades de los agentes.

Regístrese una vez y reutilícelo en todas partes

La conexión de un proveedor a AWS Security Agent implica dos pasos distintos que se producen en diferentes niveles:

1. Registre la integración (a nivel de cuenta). El proveedor se registra una vez desde la página de integraciones de la consola de administración de AWS Security Agent. Un registro representa la conexión autorizada a una cuenta de proveedor, como una GitHub organización, un GitLab grupo, un espacio de trabajo de Bitbucket o un sitio de Confluence. Los registros son recursos a nivel de cuenta.
2. Conecta los recursos a un espacio de agente (nivel de espacio de agente). Desde un espacio de agente, puedes conectar los recursos de una integración registrada (repositorios para proveedores de código fuente o páginas para Confluence) y configurar cómo los usa el agente. Este paso es específico de cada espacio de agente.

Se reutiliza un único registro en todos los espacios de agente de su cuenta. Si registró un proveedor al configurar un espacio de agente, ese mismo registro estará disponible cuando conecte los recursos a otro espacio de agente; no tendrá que volver a registrar el mismo proveedor.

Una conexión, compartida entre las distintas capacidades

Cuando se conecta un recurso a un espacio de agente, ese recurso se comparte entre las capacidades del agente. No se conecta un repositorio por separado para cada capacidad.

- El acceso de lectura se otorga al conectar el recurso. La conexión de un repositorio permite a AWS Security Agent leerlo para realizar escaneos de código completos (revisión del código), contexto de pruebas de penetración, modelado de amenazas y revisión del diseño. Conectar una página de Confluence permite al agente leerla para contextualizar la documentación en revisiones de diseño, modelos de amenazas y pruebas de penetración.
- Las acciones de escritura son opcionales en cada repositorio. Al conectar los repositorios de código fuente a un Agent Space, también puede habilitar las acciones de escritura para cada repositorio:
  - Comentarios sobre la revisión del código: el agente de seguridad de AWS publica los resultados de la revisión como comentarios en las solicitudes de extracción (o las solicitudes de fusión GitLab).

- Corrección de código: AWS Security Agent abre solicitudes de cambios (o solicitudes de fusión) con correcciones para las vulnerabilidades descubiertas.

  Estas acciones de escritura no están disponibles para los repositorios públicos. Read-only el análisis sigue siendo válido.

> **Note**
>
> Confluence es un proveedor de documentación y no un proveedor de código fuente. AWS Security Agent lee las páginas de Confluence conectadas para proporcionar contexto para las revisiones de diseño, el modelado de amenazas y las pruebas de penetración. Al seleccionar una página, se otorga acceso de lectura; no hay cambios de capacidad por página.

Proveedores compatibles

AWS Security Agent es compatible con los siguientes proveedores:

- Código fuente: GitHub (GitHub empresa alojada en la nube GitHub y alojada en la nube), servidor GitHub empresarial (autohospedado), (hospedado en la nube), GitLab GitLab Self-Managed (autohospedado) y Bitbucket Cloud.
- Documentación: Confluence Cloud.

En el caso de los proveedores autohospedados a los que no se pueda acceder a través de la Internet pública, puedes enrutar el tráfico del agente a través de una conexión privada. Para obtener más información, consulte the section called “Conéctese al control de código fuente alojado de forma privada”.

Siguientes pasos

- Registra un proveedor desde la página de integraciones. Consulte el tema de conexión de su proveedor, por ejemplo. the section called “Connect AWS Security Agent a los GitHub repositorios”
- Conecte los recursos a un espacio de agente y configure las capacidades. Consulte the section called “Habilitar la revisión de código” y the section called “Habilitar la prueba de penetración”.

Connect AWS Security Agent a los GitHub repositorios

Conecte su agente de seguridad de AWS a GitHub los repositorios para habilitar la revisión del código, el modelado de amenazas, las pruebas de penetración y las capacidades de corrección automatizadas. AWS Security Agent es compatible con empresas alojadas en la nube GitHub y alojadas en la nube GitHub . Antes de empezar, averigüe cómo the section called “Cómo funcionan las integraciones con Agent Spaces” se reutiliza un registro en los Agent Spaces y cómo se comparte entre las distintas capacidades.

GitHub la integración sirve para varios propósitos:

> **Note**
>
> Esta página incluye información sobre empresas alojadas en la nube GitHub (github.com) y alojadas en la nube. GitHub Para ver el servidor empresarial GitHub autohospedado, consulte. the section called “Connect AWS Security Agent a un servidor GitHub empresarial”

- Revisión del código: analiza automáticamente los cambios en el código de cada solicitud de extracción de datos en función de los requisitos de seguridad de tu organización y escanea todo el repositorio bajo demanda
- Modelado de amenazas: proporcione información sobre las aplicaciones mediante el análisis del código fuente, los flujos de datos y la arquitectura
- Contexto de las pruebas de penetración: proporcione información sobre las aplicaciones para las pruebas de penetración mediante el análisis del código fuente
- Solución automática: envíe solicitudes de extracción de información con correcciones para las vulnerabilidades descubiertas durante las evaluaciones de seguridad

GitHub Para conectarse a AWS Security Agent, es necesario autorizar la GitHub aplicación AWS Security Agent para su GitHub organización o cuenta de usuario y, a continuación, registrar la conexión en la consola de AWS.

¿Cómo funciona GitHub la integración

El análisis de las solicitudes de extracción se realiza desde dentro GitHub. Tras autorizar la GitHub aplicación, conectar los repositorios y habilitar los comentarios de revisión de código en la consola de administración de AWS, AWS Security Agent escanea automáticamente los cambios en cada nueva

solicitud de extracción (un análisis diferencial solo del código modificado) y publica los resultados como comentarios de la solicitud de extracción.

Las revisiones de código completas (que escanean toda la base de código de un repositorio) se crean y ejecutan en la aplicación web AWS Security Agent, no en. GitHub

Las pruebas de penetración y el modelado de amenazas se inician en la aplicación web AWS Security Agent. Los usuarios seleccionan los repositorios conectados para proporcionar el contexto de la aplicación y especifican los dominios de destino para las pruebas de penetración. Si habilitas la corrección automática, los usuarios pueden solicitar a AWS Security Agent que corrija los hallazgos abriendo solicitudes de cambios en los repositorios conectados.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- GitHub acceso de administrador de la organización o acceso de propietario de la cuenta GitHub de usuario
- Permisos para configurar las integraciones de su espacio de agente en la consola de administración de AWS
- Conozca los repositorios que desea conectar para revisar el código, modelar las amenazas y realizar pruebas de penetración

Important

Una GitHub aplicación solo se puede instalar una vez en una GitHub cuenta u GitHub organización. Si necesita conectar la misma GitHub organización a AWS Security Agent, debe usar la misma cuenta de AWS en la que se registró la integración por primera vez.

Note

Si su organización GitHub empresarial ha habilitado las listas de IP permitidas, debe aceptar las direcciones IP permitidas en la GitHub aplicación. También puede optar por añadir automáticamente las direcciones IP a su lista de direcciones permitidas. Para obtener más información, consulte Permitir el acceso por parte de GitHub aplicaciones y Habilitar las direcciones IP permitidas en la GitHub documentación.
Las siguientes direcciones IP se utilizan para acceder a sus GitHub recursos:

- Este de EE. UU. (Norte de Virginia) (us-east-1)
  - 34.228.181.128
  - 44.219.176.187
  - 54.226.244.221
- Oeste de EE. UU. (Oregón) (us-west-2)
  - 34.212.16.133
  - 52.89.67.212
  - 54.187.135.61
- Asia-Pacífico (Mumbai) (ap-south-1)
  - 13.126.209.199
  - 13.234.6.24
  - 35.154.102.216
- Asia-Pacífico (Singapur) (ap-southeast-1)
  - 18.139.13.125
  - 47.130.240.215
  - 54.179.238.173
- Asia-Pacífico (Sídney) (ap-southeast-2)
  - 13.237.95.197
  - 13.238.84.102
  - 52.64.174.242
- Asia-Pacífico (Tokio) (ap-northeast-1)
  - 13.192.12.233
  - 35.74.181.230
  - 57.183.50.158
- Europa (Fráncfort) (eu-central-1)
  - 18.158.110.140
  - 52.57.96.160
  - 52.59.55.56
- Europa (Irlanda) (eu-west-1)
  - 34.251.85.24

    - 52.30.157.157
    - 52.51.192.222
  - América del Sur (São Paulo) (sa-east-1)
    - 54.94.247.213
    - 54.207.222.14
    - 54.232.201.242

Autorizar y registrar la GitHub aplicación AWS Security Agent

Autorice a la GitHub aplicación AWS Security Agent a acceder a su GitHub organización o cuenta de usuario y, a continuación, registre la conexión en la consola de AWS.

> **Important**
>
> Complete todos los pasos de este proceso sin cerrar el navegador ni abandonar la navegación. Si se interrumpe el proceso de registro, es posible que deba desinstalar la GitHub aplicación y empezar de nuevo.

1. En la consola de administración de AWS Security Agent, vaya a Integraciones.
2. Seleccione Add Integration.
3. Seleccione GitHub.
4. Elija Siguiente.
5. Elija Instalar y autorizar.

   Se le redirigirá GitHub a para completar la autorización. Asegúrese de haber iniciado sesión GitHub con una cuenta que tenga acceso de administrador a la cuenta de usuario o organización a la que desee conectarse.
6. En GitHub, seleccione la cuenta u organización en la que desea instalar la GitHub aplicación AWS Security Agent.
7. Seleccione los repositorios a los que puede acceder AWS Security Agent:
   - Todos los repositorios: otorga acceso a todos los repositorios actuales y futuros de la organización o cuenta de usuario

- Seleccione solo los repositorios: elija repositorios específicos en el menú desplegable. Puedes seleccionar varios repositorios de uno en uno.

> **Note**
>
> Puede modificar el acceso al repositorio en cualquier momento visitando la configuración de la GitHub aplicación en su GitHub organización o la configuración de la cuenta de usuario.

8. Selecciona Instalar y autorizar.
9. Se le redirigirá de nuevo a la consola de administración de AWS para completar el registro.
10. En la sección Detalles de registro, configure los siguientes campos:
    a. Nombre de registro: introduzca un nombre descriptivo para esta GitHub conexión. Utilice un nombre que identifique la GitHub organización o la cuenta de usuario, como «Acme-Corp-Org» o «Production-Repos».
    b. Tipo de cuenta: seleccione una de las siguientes opciones en el menú desplegable:
       - Organización: si has conectado una cuenta de GitHub organización
       - Usuario: si ha conectado una cuenta GitHub de usuario personal
    c. Nombre de la organización (aparece solo si ha seleccionado Organización): introduzca el nombre exacto de su GitHub organización tal y como aparece en GitHub.
11. Elija Conectar.
12. Aparece un mensaje de confirmación y regresa a la página de integraciones, donde aparece la nueva GitHub conexión con su nombre de registro. Para conectar otras GitHub organizaciones o cuentas de usuario, repita este proceso y vuelva a seleccionar Añadir integración.

Solucione problemas de integración GitHub

Si encuentra problemas durante el proceso de GitHub integración, utilice las siguientes instrucciones para resolver los problemas más comunes.

No se ha podido completar el registro

Si no pudo completar el proceso de registro (por ejemplo, se cerró el navegador, salió de la página de registro o se produjo una interrupción en la sesión), es posible que la GitHub aplicación AWS Security Agent esté instalada en su GitHub organización pero no esté registrada en la consola de AWS.

Síntomas:

- Cuando intenta volver a autorizar la GitHub aplicación, GitHub aparece «Configurar» en lugar de «Instalar»
- No puede completar el registro en la consola de AWS
- La integración no aparece en su lista de integraciones

Solución:

1. Desinstale la GitHub aplicación AWS Security Agent de su GitHub organización o cuenta de usuario.
2. Regrese a la consola de AWS Security Agent y vuelva a iniciar el proceso de integración desde el principio.

Varias cuentas de AWS que intentan integrar la misma GitHub organización

Una GitHub aplicación solo se puede instalar una vez en una GitHub cuenta u GitHub organización. Si necesita usar repositorios de una GitHub organización que ya está integrada con otra cuenta de AWS Security Agent, debe usar la cuenta de AWS en la que se registró la integración por primera vez.

Solución:

- Identifique qué cuenta de AWS Security Agent tiene registrada la GitHub integración
- Use esa cuenta de AWS para crear espacios de agentes y conectar repositorios
- Si necesita mover la integración a una cuenta de AWS diferente, desinstale primero la GitHub aplicación de la cuenta de AWS original y, a continuación, intégrela con la nueva cuenta

Siguientes pasos

Tras conectarse GitHub a AWS Security Agent:

- Navegue hasta el espacio de agentes en el que desee utilizar estos repositorios
- Seleccione Habilitar la revisión de código o Configurar pruebas de penetración para conectar repositorios específicos a su espacio de agente y configurar su uso
- Habilite la corrección automática para permitir que AWS Security Agent envíe solicitudes de cambios con correcciones de vulnerabilidades

- Revise los permisos de las GitHub aplicaciones y el acceso a los repositorios en la configuración de su GitHub organización

Eliminar una GitHub integración

Elimine una GitHub integración cuando ya no necesite que AWS Security Agent acceda a los repositorios desde una GitHub organización o cuenta de usuario específica. Primero debe desinstalar la GitHub aplicación AWS Security Agent GitHub antes de eliminar la integración en la consola de AWS.

Requisitos previos para la eliminación

Antes de eliminar una GitHub integración, asegúrese de tener:

- Ha comprobado qué espacios de agentes tienen repositorios conectados desde esta integración
- Comprendió el impacto: eliminar esta integración interrumpiría las conexiones de los repositorios para la revisión del código, el contexto de las pruebas de penetración y la corrección de las pruebas de penetración en todos los espacios de agente que utilizan los repositorios de esta integración
- GitHub acceso del administrador de la organización o acceso del propietario de la cuenta de usuario para desinstalar la aplicación GitHub

Paso 1: desinstale la GitHub aplicación AWS Security Agent de GitHub

En primer lugar, desinstale la GitHub aplicación AWS Security Agent de su GitHub organización o cuenta de usuario.

Para GitHub Organizations:

1. Ve a github.com y abre la página de tu organización.
2. En la barra lateral izquierda, selecciona Configuración.
3. En Código, planificación y automatización, selecciona Aplicaciones instaladas GitHub .
4. Localice la aplicación AWS Security Agent en la lista.
5. Elija Configurar junto a la aplicación AWS Security Agent.
6. Desplácese hasta la parte inferior de la página de configuración y seleccione Desinstalar.
7. Confirme la desinstalación cuando se le solicite.

Para cuentas GitHub de usuario:

1. Ve a github.com.
2. Elige tu foto de perfil.
3. Seleccione Configuración.
4. En la barra lateral izquierda, selecciona Aplicaciones.
5. Abre la pestaña GitHub Aplicaciones instaladas.
6. Localice la aplicación AWS Security Agent en la lista.
7. Elija Configurar junto a la aplicación AWS Security Agent.
8. Desplácese hasta la parte inferior de la página de configuración y seleccione Desinstalar.
9. Confirme la desinstalación cuando se le solicite.

Paso 2: Eliminar la integración de AWS Security Agent

Tras desinstalar la GitHub aplicación, elimine el registro de integración de la consola de AWS.

1. En la consola de administración de AWS Security Agent, vaya a Integraciones.
2. Busque la GitHub integración que desee eliminar en la lista de integraciones.
3. Selecciona la integración haciendo clic en ella.
4. Elija Eliminar .
5. Revise el cuadro de diálogo de confirmación, que le avisa sobre el impacto:

> **Warning**
>
> La eliminación de esta integración afectará a todos los espacios de agentes que tengan repositorios conectados desde esta GitHub organización o cuenta de usuario. Esto interrumpirá:
>
> - Funcionalidad de revisión de código para los repositorios conectados
> - Contexto de pruebas de penetración desde repositorios conectados
> - Capacidades de corrección de pruebas de penetración para repositorios conectados
>
> Asegúrese de haber desinstalado la GitHub aplicación AWS Security Agent GitHub antes de continuar.

6. Si aún no ha desinstalado la GitHub aplicación desde GitHub, recibirá una advertencia. Vuelva al paso 1 para completar primero la desinstalación.

7. Si has desinstalado la GitHub aplicación y entiendes las consecuencias, selecciona Confirmar la eliminación.
8. La integración se elimina de la lista de integraciones. Los Agent Spaces con repositorios de esta integración ya no tienen acceso a esos repositorios para revisar el código, contextualizar las pruebas de penetración o realizar correcciones automatizadas.

Connect AWS Security Agent a los GitLab repositorios

Conecte su agente de seguridad de AWS a los repositorios GitLab en la nube para habilitar las funciones de revisión de código, modelado de amenazas, pruebas de penetración y corrección automatizada. Antes de empezar, compruebe cómo se reutiliza un registro en los Agent Spaces y cómo se comparte entre las distintas capacidades. the section called “Cómo funcionan las integraciones con Agent Spaces”

GitLab la integración sirve para varios propósitos:

- Revisión del código: analice automáticamente los cambios de código de cada solicitud de fusión en función de los requisitos de seguridad de su organización y realice escaneos de todo el repositorio bajo demanda
- Modelado de amenazas: proporcione información sobre las aplicaciones mediante el análisis del código fuente, los flujos de datos y la arquitectura
- Contexto de las pruebas de penetración: proporcione información sobre las aplicaciones para las pruebas de penetración mediante el análisis del código fuente
- Solución automática: envíe solicitudes de fusión con correcciones para las vulnerabilidades descubiertas durante las evaluaciones de seguridad

GitLab Para conectarse a AWS Security Agent, es necesario proporcionar un token de GitLab acceso con los permisos adecuados y, a continuación, registrar la conexión en la consola de AWS.

¿Cómo funciona GitLab la integración

El análisis de las solicitudes de fusión se realiza internamente GitLab. Tras proporcionar su token de acceso, conectar los proyectos y habilitar los comentarios de revisión de código en la consola de administración de AWS, AWS Security Agent escanea automáticamente los cambios en cada nueva solicitud de fusión (un análisis diferencial solo del código modificado) y publica los resultados como comentarios de la solicitud de fusión.

Puede crear y ejecutar revisiones de código completas (que escanean toda la base de código de un proyecto) en la aplicación web AWS Security Agent, no en. GitLab

Las pruebas de penetración y el modelado de amenazas se inician en la aplicación web AWS Security Agent. Los usuarios especifican los dominios de destino y seleccionan los repositorios conectados para proporcionar el contexto de la aplicación. Si habilita la corrección automática, los usuarios pueden solicitar a AWS Security Agent que corrija los hallazgos abriendo solicitudes de fusión en los repositorios conectados.

> **Note**
>
> La corrección automática no está disponible para los GitLab repositorios públicos a fin de evitar que se revelen las vulnerabilidades antes de que se solucionen.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Una GitLab.com cuenta con acceso de mantenedor o propietario a los proyectos a los que quieras conectarte
- Un token de GitLab acceso con los alcances necesarios para tu tipo de conexión:
  - Personal: un token de acceso personal con todos los permisos de lectura y el `api` permiso.
  - Grupo: un token de acceso grupal con los `read_repository` ámbitos `read_api` y.
- Permisos para configurar las integraciones en la consola de administración de AWS Security Agent

> **Important**
>
> Establezca la caducidad del token en un máximo de 365 días a partir de la fecha actual.

> **Note**
>
> GitLab Los tokens de acceso personal se pueden usar en varias cuentas de AWS. A diferencia GitHub de las integraciones de Atlassian, no hay restricciones a la hora de conectar la misma GitLab cuenta a varias instancias de AWS Security Agent.

Registre una conexión GitLab

1. En la consola de administración de AWS Security Agent, vaya a Integraciones.
2. Seleccione Add Integration.
3. Seleccione GitLaby, a continuación, elija Siguiente.
4. En Elige un tipo de cuenta, selecciona una de las siguientes opciones:
   - Personal: conecta tu cuenta GitLab de usuario individual.
   - Grupo: conecta un GitLab grupo que contenga varios proyectos. Introduce tu ID de grupo.
5. En el campo Token de acceso, pega tu token de GitLab acceso.
6. En el campo Nombre de registro, introduce un nombre descriptivo para esta conexión, por ejemplo`Engineering-Team-GitLab`. Los caracteres válidos son letras, números, puntos, guiones bajos y guiones.
7. Elija Conectar.

   Vuelve a la página de integraciones, donde aparece la nueva conexión con su nombre de registro.

Solucionar problemas de integración GitLab

Si encuentra problemas durante el proceso de GitLab integración, utilice las siguientes instrucciones para resolver los problemas más comunes.

El token no es válido o ha caducado

Síntomas

- La integración no se puede conectar
- La integración que funcionaba anteriormente deja de funcionar
- Mensaje de error que indica un error de autenticación

Resolución

1. En GitLab, vaya a la configuración de usuario y seleccione Tokens de acceso.
2. Verifica que tu token no haya caducado.
3. Comprueba que el token tenga los alcances necesarios para su tipo.
4. Si el token ha caducado, cree uno nuevo y actualice la integración en la consola de AWS.

Limitación de tasas

Síntomas

- Fallos intermitentes durante la revisión del código
- Análisis retrasado de las solicitudes de fusión

Resolución

- GitLab aplica límites de velocidad a las solicitudes de API. Si tienes una gran cantidad de repositorios o solicitudes de fusión frecuentes, es posible que algunas solicitudes estén limitadas.
- Espera a que se restablezca el límite de velocidad o ponte en contacto con el servicio de GitLab asistencia para aumentar tus límites de velocidad.

Siguientes pasos

Tras conectarse GitLab a AWS Security Agent:

- Navegue hasta el espacio de agentes en el que desee utilizar estos repositorios
- Seleccione Habilitar la revisión del código o Configurar las pruebas de penetración para conectar proyectos específicos a su espacio de agente y configurar su uso
- Habilite la corrección de código para permitir que AWS Security Agent envíe solicitudes de fusión con correcciones de vulnerabilidades
- Para ver las GitLab instancias alojadas de forma privada, consulte the section called “Conecta AWS Security Agent a GitLab Self-Managed”

Conecta AWS Security Agent a GitLab Self-Managed

Conecte su AWS Security Agent a una GitLab Self-Managed instancia para habilitar la revisión del código, el modelado de amenazas, las pruebas de penetración y las capacidades de corrección automatizadas para los repositorios alojados en su propia infraestructura.

GitLab Self-Managed La integración funciona igual que en la GitLab nube (consultethe section called “Connect AWS Security Agent a los GitLab repositorios”), con una configuración adicional para la conectividad de red con su instancia privada. Antes de empezar, compruebe cómo se reutiliza un registro en los Agent Spaces y cómo se comparte entre las distintas capacidades. the section called “Cómo funcionan las integraciones con Agent Spaces”

> **Note**
>
> GitLab Self-Managed se registra mediante la GitLabintegración, no mediante un tipo de integración independiente. En el flujo de registro, selecciona Usar punto de conexión GitLab autohospedado y proporciona la URL de la instancia. El GitLab flujo alojado en la nube se describe en. the section called “Connect AWS Security Agent a los GitLab repositorios”

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Una GitLab Self-Managed instancia que es una de las siguientes:
  - Accesible públicamente a través de Internet, O
  - Accesible a través de una conexión privada (consultethe section called “Conéctese al control de código fuente alojado de forma privada”)
- Un token de GitLab acceso con los alcances necesarios para tu tipo de conexión:
  - Personal: un token de acceso personal con todos los permisos de lectura y el `api` permiso.
  - Grupo: un token de acceso grupal con los `read_repository` ámbitos `read_api` y.
- Acceso de mantenedor o propietario a los proyectos a los que quieres conectarte
- La GitLab instancia debe ofrecer tráfico HTTPS con una versión TLS mínima de 1.2

> **Note**
>
> Si tu GitLab Self-Managed instancia usa certificados TLS emitidos por una entidad de certificación privada, puedes proporcionar la clave PEM-encoded pública del certificado al crear una conexión privada. Esto permite que AWS Security Agent confíe en la conexión TLS de su instancia.

Registre una conexión GitLab Self-Managed

1. En la consola de administración de AWS Security Agent, vaya a Integraciones.
2. Seleccione Add Integration.
3. Seleccione GitLaby, a continuación, elija Siguiente.

4. En Elige un tipo de cuenta, selecciona Personal o Grupo. Si seleccionas Grupo, introduce tu ID de grupo.
5. Selecciona Usar punto de conexión GitLab autohospedado.
6. En el campo URL del punto de conexión GitLab autohospedado, introduce la URL de tu instancia, por ejemplo. `https://gitlab.example.com`
7. Si su instancia no es de acceso público, seleccione Conectar al punto final mediante una conexión privada y, a continuación, elija una conexión privada existente o cree una nueva. Consulte the section called “Conéctese al control de código fuente alojado de forma privada”.
8. En el campo Token de acceso, pega tu token de GitLab acceso.
9. En el campo Nombre de registro, introduce un nombre descriptivo para esta conexión. Los caracteres válidos son letras, números, puntos, guiones bajos y guiones.
10. Elija Conectar.

    Vuelve a la página de integraciones, donde aparece la nueva conexión con su nombre de registro.

Conectividad privada

Si su GitLab Self-Managed instancia no es de acceso público, debe crear una conexión privada antes de registrar la integración. Consulte the section called “Conéctese al control de código fuente alojado de forma privada” para obtener instrucciones detalladas.

> **Important**
>
> Service-managed las conexiones privadas requieren que la GitLab Self-Managed instancia se ejecute en la misma cuenta de AWS en la que se creó el espacio de agentes. Para el acceso entre cuentas, utilice una conexión privada autogestionada en la que proporcione su propia configuración de recursos de VPC Lattice.

GitLab Self-Managed Solucione los problemas de integración

Además de los pasos de solución de problemasthe section called “Connect AWS Security Agent a los GitLab repositorios”, los siguientes problemas son específicos de las instancias autogestionadas:

Instancia inalcanzable

Síntomas

- La conexión falla debido al tiempo de espera o a un error de red
- La integración funcionaba anteriormente, pero deja de funcionar

Resolución

- Compruebe que la GitLab instancia esté en ejecución y sea accesible
- Si utilizas una conexión privada, verifica que la puerta de enlace de recursos de VPC Lattice esté en buen estado y que los ENI tengan conectividad de red con tu instancia
- Verifica que los grupos de seguridad permitan el tráfico en el puerto configurado
- Compruebe que el certificado TLS sea válido y no haya caducado

Errores en el certificado TLS

Síntomas

- La conexión falla debido a un SSL/TLS error

Resolución

- Verifica que la instancia sirva HTTPS con TLS 1.2 o una versión superior
- Si utilizas una entidad de certificación privada, asegúrate de que la clave PEM-encoded pública se haya proporcionado durante la configuración de la conexión privada
- Compruebe que el certificado no esté caducado

Siguientes pasos

Tras conectarse GitLab Self-Managed a AWS Security Agent:

- Navegue hasta el espacio de agentes en el que desee utilizar estos repositorios
- Seleccione Habilitar la revisión de código o Configurar pruebas de penetración para conectar proyectos específicos
- Habilite la corrección de código para las correcciones basadas en solicitudes de fusión

Eliminar una GitLab integración

Elimine una GitLab integración cuando ya no necesite que AWS Security Agent acceda a los repositorios desde una GitLab cuenta o un grupo específicos.

Requisitos previos para la eliminación

Antes de eliminar una GitLab integración, asegúrese de tener:

- Comprobó qué espacios de agentes tienen repositorios conectados desde esta integración
- Comprendió el impacto: eliminar esta integración interrumpiría las conexiones entre los repositorios para la revisión del código, el contexto de las pruebas de penetración, el modelado de amenazas y la corrección automática en todos los espacios de agente que utilizan los repositorios de esta integración

Eliminar la integración de AWS Security Agent

1. En la consola de administración de AWS Security Agent, vaya a Integraciones.
2. Localice la GitLab integración que desee eliminar.
3. Selecciona la integración haciendo clic en ella.
4. Elija Eliminar .
5. Revise el cuadro de diálogo de confirmación y seleccione Confirmar la eliminación.

> **Note**
>
> Tras eliminar la integración, es posible que también desees revocar el token de acceso personal para impedir GitLab que sigas accediendo a él. Ve a la configuración GitLab de usuario y elimina o revoca el token.

El mismo proceso se aplica a las GitLab Self-Managed integraciones.

Connect AWS Security Agent a un servidor GitHub empresarial

Conecte su AWS Security Agent a una instancia de GitHub Enterprise Server (GHES) para habilitar la revisión del código, el modelado de amenazas, las pruebas de penetración y las capacidades de corrección automatizadas para los repositorios alojados en su propia infraestructura.

GitHub La integración de servidores empresariales proporciona las mismas capacidades que la alojada en la nube GitHub (consulte Conectar AWS Security Agent a GitHub los repositorios) con una configuración adicional para la conectividad de red con la instancia autohospedada. Antes de empezar, compruebe cómo se reutiliza un registro en los Agent Spaces y cómo se comparte entre las distintas capacidades. the section called “Cómo funcionan las integraciones con Agent Spaces”

> **Note**
>
> GitHub Enterprise Server se registra mediante la GitHubintegración, no como un tipo de integración independiente. En el flujo de registro, se elige GitHub Enterprise Server como tipo de instancia. El GitHub.com flujo alojado en la nube se describe enthe section called “Connect AWS Security Agent a los GitHub repositorios”.

Cómo funciona GitHub la integración de Enterprise Server

El análisis de las solicitudes de extracción se realiza en GitHub Enterprise Server. Tras autorizar la conexión, conectar los repositorios y habilitar los comentarios de revisión de código en la consola de administración de AWS, AWS Security Agent escanea automáticamente los cambios en cada nueva solicitud de extracción (un análisis diferencial solo del código modificado) y publica los resultados como comentarios de la solicitud de extracción.

Puede crear y ejecutar revisiones de código completas (que escanean toda la base de código de un repositorio) en la aplicación web AWS Security Agent, no en GitHub Enterprise Server.

Las pruebas de penetración y el modelado de amenazas se inician en la aplicación web AWS Security Agent. Los usuarios especifican los dominios de destino y seleccionan los repositorios conectados para proporcionar el contexto de la aplicación. Si habilitas la corrección automática, los usuarios pueden solicitar a AWS Security Agent que corrija los hallazgos abriendo solicitudes de cambios en los repositorios conectados.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Una instancia GitHub de Enterprise Server que sea:
  - Accesible públicamente a través de Internet, O
  - Accesible a través de una conexión privada (consultethe section called “Conéctese al control de código fuente alojado de forma privada”)

- Acceso de administrador del sitio o administrador de la organización a su instancia de GHES
- La instancia de GHES debe atender el tráfico HTTPS con una versión TLS mínima de 1.2
- Permisos para configurar las integraciones en la consola de administración de AWS Security Agent

> **Note**
>
> GitHub Las integraciones de Enterprise Server se pueden utilizar en varias cuentas de AWS.

Registre una conexión a GitHub Enterprise Server

El registro de una conexión de GitHub Enterprise Server utiliza un flujo de OAuth-based autorización.

> **Important**
>
> Complete todos los pasos de este proceso sin cerrar el navegador ni navegar. Si se interrumpe el proceso de registro, es posible que tenga que reiniciarlo desde el principio.

1. En la consola de administración de AWS Security Agent, vaya a Integraciones.
2. Seleccione Add Integration.
3. Seleccione GitHuby, a continuación, elija Siguiente.
4. En Tipo de instancia, selecciona GitHub Enterprise Server.
5. En el campo URL de GitHub Enterprise Server, introduce la URL HTTPS de tu instancia, por ejemplo`https://github.example.com`.
6. Si su instancia no es de acceso público, seleccione Conectar al punto final mediante una conexión privada y, a continuación, elija una conexión privada existente o cree una nueva. Consulte the section called “Conéctese al control de código fuente alojado de forma privada”.
7. En la sección Detalles del registro, configura los siguientes campos:
   a. Nombre de registro: introduzca un nombre descriptivo para esta conexión. Los caracteres válidos son letras, números, puntos, guiones bajos y guiones.
   b. GitHub tipo de cuenta: seleccione la organización o el usuario.
   c. Nombre de la organización (aparece solo si ha seleccionado Organización): introduzca el nombre exacto de su organización de GitHub Enterprise Server. Los nombres distinguen mayúsculas de minúsculas.

8. Elija Conectar.

> **Note**
>
> AWS Security Agent lo redirige fuera de la consola para completar la autorización con su instancia de GitHub Enterprise Server. Una vez completada la autorización, vuelve a la consola y la nueva conexión aparece en la página de integraciones.

Conectividad privada

Si su instancia de GitHub Enterprise Server no es de acceso público, debe crear una conexión privada antes de registrar la integración. Consulte the section called “Conéctese al control de código fuente alojado de forma privada” para obtener instrucciones detalladas.

> **Important**
>
> Service-managed las conexiones privadas requieren que la instancia de GHES se ejecute en la misma cuenta de AWS en la que se creó el espacio de agentes. Para el acceso entre cuentas, utilice una conexión privada autogestionada.

> **Note**
>
> Si la instancia de GHES usa certificados TLS emitidos por una entidad de certificación privada, proporcione la clave PEM-encoded pública del certificado al crear la conexión privada.

Solucione los problemas de integración de GitHub Enterprise Server

Si tiene problemas para conectar AWS Security Agent a GitHub Enterprise Server, utilice las siguientes instrucciones para diagnosticar y resolver problemas frecuentes.

Error de redireccionamiento de OAuth

Síntomas

- Los redireccionamientos del navegador fallan durante el flujo de autorización

- Se muestra una página de error después de autorizar en el GHES

Resolución

- Compruebe que se pueda acceder a la instancia de GHES desde el navegador
- Asegúrese de que la URL de devolución de llamada de OAuth esté configurada correctamente
- Reinicie el proceso de integración desde el principio

Instancia inalcanzable

Síntomas

- La conexión falla debido al tiempo de espera o a un error de red

Resolución

- Compruebe que la instancia de GHES esté en ejecución y sea accesible
- Si utilizas una conexión privada, verifica la conectividad de VPC Lattice
- Compruebe que los grupos de seguridad permitan el tráfico en el puerto configurado
- Compruebe que el certificado TLS sea válido (TLS 1.2 como mínimo)

Siguientes pasos

Tras conectar GitHub Enterprise Server a AWS Security Agent:

- Navegue hasta el espacio de agentes en el que desee utilizar estos repositorios
- Seleccione Habilitar la revisión de código o Configurar pruebas de penetración para conectar repositorios específicos
- Habilite la corrección de código para permitir que AWS Security Agent envíe solicitudes de cambios con correcciones de vulnerabilidades

Eliminar una integración GitHub de Enterprise Server

Elimine la integración de un servidor GitHub empresarial cuando ya no necesite AWS Security Agent para acceder a los repositorios desde una instancia de GHES específica.

Requisitos previos para la eliminación

Antes de eliminar una integración de GHES:

- Compruebe qué espacios de agentes tienen repositorios conectados desde esta integración
- Comprenda el impacto: eliminarlo no funcionará: la revisión del código, el contexto de las pruebas de penetración, el modelado de amenazas y la remediación automática de todos los repositorios conectados

Elimine la integración

1. En la consola de administración de AWS Security Agent, vaya a Integraciones.
2. Localice la integración de GitHub Enterprise Server que desee eliminar.
3. Seleccione la integración.
4. Elija Eliminar .
5. Revise el cuadro de diálogo de confirmación y seleccione Confirmar la eliminación.

> **Note**
>
> Tras la eliminación, es posible que también desees revocar la aplicación OAuth en tu instancia de GHES. Ve a la configuración de tu organización de GHES y elimina la aplicación autorizada.

Encuentra tu ID de instalación de Atlassian

Antes de registrar una integración de Bitbucket o Confluence en la consola de AWS, debes encontrar el ID de instalación en la aplicación AWS Security Agent Forge instalada en tu sitio de Atlassian. Debe pegar este ID en el flujo de registro.

Para Bitbucket

1. En Bitbucket, navega hasta la configuración de tu espacio de trabajo.
2. Selecciona Forge Apps en la barra lateral.
3. Busque Connect with AWS Security Agent en la lista de aplicaciones instaladas.

4. Seleccione Copiar al portapapeles para copiar el ID de instalación.

Para Confluence

1. En Confluence, dirígete a la administración de Confluence.
2. Selecciona Aplicaciones en la barra lateral.
3. Busque Connect with AWS Security Agent en la lista de aplicaciones instaladas.
4. Seleccione Copiar al portapapeles para copiar el ID de instalación.

Necesitará este identificador de instalación al completar el registro en la consola de administración de AWS Security Agent.

Connect AWS Security Agent a los repositorios de Bitbucket

Conecta tu AWS Security Agent a los repositorios de Bitbucket Cloud para habilitar las funciones de revisión de código, modelado de amenazas, pruebas de penetración y remediación automatizada. Antes de empezar, compruébelo the section called “Cómo funcionan las integraciones con Agent Spaces” para comprender cómo se reutiliza un registro en los espacios de agente y cómo se comparte entre las distintas capacidades.

La integración de Bitbucket sirve para varios propósitos:

- Revisión del código: analiza automáticamente los cambios en el código de cada solicitud de extracción de datos en función de los requisitos de seguridad de tu organización y escanea todo el repositorio bajo demanda
- Modelado de amenazas: proporcione información sobre las aplicaciones mediante el análisis del código fuente, los flujos de datos y la arquitectura
- Contexto de las pruebas de penetración: proporcione información sobre las aplicaciones para las pruebas de penetración
- Solución automática: envíe solicitudes de extracción de información con correcciones para las vulnerabilidades descubiertas durante las evaluaciones de seguridad

Para conectar Bitbucket a AWS Security Agent, es necesario instalar la aplicación AWS Security Agent Forge en tu sitio de Atlassian y completar el flujo de autorización de OAuth.

> **Note**
>
> AWS Security Agent solo es compatible con Bitbucket Cloud. El servidor de Bitbucket y el centro de datos de Bitbucket no son compatibles.

Cómo funciona la integración de Bitbucket

El análisis de las solicitudes de extracción se realiza en Bitbucket. Tras instalar la aplicación Forge, conectar los repositorios y habilitar los comentarios de revisión de código en la consola de administración de AWS, AWS Security Agent escanea automáticamente los cambios en cada nueva solicitud de extracción (un análisis diferencial solo del código modificado) y publica los resultados como comentarios de la solicitud de extracción.

Las revisiones de código completas (que escanean toda la base de código de un repositorio) se crean y ejecutan en la aplicación web AWS Security Agent, no en Bitbucket.

Las pruebas de penetración y el modelado de amenazas se inician en la aplicación web AWS Security Agent. Los usuarios especifican los dominios de destino y seleccionan los repositorios conectados para proporcionar el contexto de la aplicación.

> **Note**
>
> La corrección automática no está disponible en los repositorios públicos de Bitbucket para evitar revelar las vulnerabilidades antes de que se solucionen.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Un espacio de trabajo de Bitbucket Cloud con acceso de administrador
- Una cuenta de Atlassian con privilegios de administrador del sitio
- Permisos para configurar las integraciones en la consola de administración de AWS Security Agent

> **Important**
>
> Un sitio de Atlassian solo se puede asociar a una cuenta de AWS por región. Si necesitas conectar el mismo sitio de Bitbucket a AWS Security Agent en una cuenta de AWS diferente dentro de la misma región, primero debes eliminar la integración existente.

> **Note**
>
> El precio de la aplicación Atlassian Forge se aplica a esta integración. Para obtener más información, consulta los precios de la plataforma Forge en la documentación de Atlassian.

Registra una conexión a Bitbucket

1. En la consola de administración de AWS Security Agent, vaya a Integraciones.
2. Seleccione Add Integration.
3. Selecciona Bitbucket y, a continuación, selecciona Siguiente.
4. Instale la aplicación AWS Security Agent Forge en su espacio de trabajo de Bitbucket siguiendo las instrucciones que aparecen en pantalla. Tras la instalación, copia el ID de instalación. Consulte the section called “Encuentra tu ID de instalación de Atlassian”.
5. En el campo ID de instalación, pega el ID de instalación que copiaste de Bitbucket.
6. En el campo del espacio de trabajo de Bitbucket, introduce el slug del espacio de trabajo de Bitbucket, por ejemplo. `acme-corp`
7. Seleccione Autorizar.

   Se te redirigirá a Atlassian para autorizar a AWS Security Agent a acceder a tu espacio de trabajo de Bitbucket. Una vez completada la autorización, volverás a la consola.
8. En la sección Detalles del registro, introduzca un nombre de registro para esta conexión. Los caracteres válidos son letras, números, puntos, guiones bajos y guiones.
9. Elija Conectar.

> **Note**
>
> Retraso de aprovisionamiento después de la conexión

Tras elegir Connect, el aprovisionamiento por parte de Atlassian puede tardar unos minutos. Durante este tiempo, la integración informa de que está pendiente. Si intentas seleccionar repositorios o habilitar la revisión del código antes de que se complete el aprovisionamiento, es posible que veas un mensaje que indica que la instalación aún no está disponible. Espere unos minutos e inténtelo de nuevo.

Soluciona problemas de integración de Bitbucket

Si tienes problemas durante el proceso de integración de Bitbucket, sigue las siguientes instrucciones para resolver los problemas más comunes.

No se ha podido completar el registro

Si se interrumpe el proceso de registro (se cierra el navegador, se agota el tiempo de espera de la sesión), es posible que la aplicación Forge esté instalada en tu sitio de Atlassian pero no esté registrada en la consola de AWS.

Resolución

- Regrese a la consola de AWS Security Agent y reinicie el proceso de integración.
- La aplicación Forge permanece instalada y no es necesario volver a instalarla.

El sitio ya está conectado a otra cuenta de AWS

Síntomas

- Error al indicar que el sitio de Atlassian ya está asociado a otra cuenta

Resolución

- Un sitio de Atlassian solo se puede conectar a una cuenta de AWS por región.
- Identifique qué cuenta de AWS tiene la integración existente y utilícela o elimine primero la integración existente.

La instalación no está disponible

Síntomas

- Cuando seleccionas repositorios o habilitas la revisión del código, aparece un mensaje que indica que la instalación de Bitbucket está en estado`PENDING_INSTALLATION`, no. `AVAILABLE`

Resolución

- La instalación sigue aprovisionándose en el lado de Atlassian. El aprovisionamiento normalmente se completa en unos minutos. Espere unos minutos e inténtelo de nuevo.
- Si el estado no está disponible después de varios minutos, elimine la integración y vuelva a registrarla. Antes de volver a registrarte, desinstala la aplicación Forge de tu espacio de trabajo de Bitbucket. Para obtener instrucciones, consulta Eliminar una integración de Bitbucket. Si vuelves a registrarte sin desinstalar la aplicación Forge anterior, la instalación puede quedar atascada en un estado pendiente.

Siguientes pasos

Tras conectar Bitbucket a AWS Security Agent:

- Navegue hasta el espacio de agentes en el que desee usar estos repositorios
- Seleccione Habilitar la revisión de código o Configurar pruebas de penetración para conectar repositorios específicos a su espacio de agente
- Habilite la corrección de código para permitir que AWS Security Agent envíe solicitudes de cambios con correcciones de vulnerabilidades

Eliminar una integración de Bitbucket

Elimine una integración de Bitbucket cuando ya no necesite AWS Security Agent para acceder a los repositorios desde un espacio de trabajo de Bitbucket específico.

Requisitos previos para la eliminación

Antes de eliminar una integración de Bitbucket:

- Comprueba qué Agent Spaces tienen repositorios conectados desde esta integración

- Comprenda el impacto: eliminarlo no funcionará: la revisión del código, el contexto de las pruebas de penetración, el modelado de amenazas y la remediación automática de todos los repositorios conectados

Paso 1: Eliminar la integración de AWS Security Agent

1. En la consola de administración de AWS Security Agent, vaya a Integraciones.
2. Localice la integración de Bitbucket que desee eliminar.
3. Selecciona la integración.
4. Elija Eliminar .
5. Revise el cuadro de diálogo de confirmación y seleccione Confirmar la eliminación.

Paso 2: desinstala la aplicación Forge

Tras eliminar la integración de AWS Security Agent, desinstala la aplicación Forge de tu sitio de Atlassian:

1. En Bitbucket, dirígete a la configuración del espacio de trabajo.
2. Selecciona Forge Apps.
3. Localice Connect with AWS Security Agent.
4. Elija Desinstalar.

> **Important**
>
> La aplicación Forge no se desinstala automáticamente
>
> Al eliminar la integración en la consola de AWS Security Agent, no se desinstala la aplicación Forge del sitio de Atlassian. Si tienes pensado volver a registrar el mismo espacio de trabajo de Bitbucket, primero debes desinstalar la aplicación Forge. De lo contrario, la nueva instalación puede quedar atascada en un estado pendiente.

Conecta el agente de seguridad de AWS a Confluence

Conecta tu agente de seguridad de AWS a Confluence Cloud para proporcionar el contexto de la documentación para las evaluaciones de seguridad. A diferencia de los proveedores de código, Confluence sirve como fuente de documentación que proporciona modelos de amenazas, documentos de arquitectura, especificaciones de API y otros materiales que mejoran la calidad de las revisiones de seguridad. Antes de empezar, compruébelo the section called “Cómo funcionan las integraciones con Agent Spaces” para comprender cómo se reutiliza un registro en los Agent Spaces.

La integración de Confluence tiene varios propósitos:

- Contexto de la revisión del diseño: proporcione documentos arquitectónicos y especificaciones de diseño para las revisiones del diseño de seguridad
- Modelado de amenazas: proporcione los modelos de amenazas existentes y la documentación del sistema para el análisis de amenazas
- Contexto de las pruebas de penetración: proporcione la documentación de la aplicación para una comprensión más profunda durante las pruebas de penetración

Para conectar Confluence a AWS Security Agent, es necesario instalar la aplicación AWS Security Agent Forge en tu sitio de Atlassian y completar el flujo de autorización de OAuth.

> **Note**
>
> AWS Security Agent solo es compatible con Confluence Cloud. No se admiten Confluence Data Center ni Confluence Server.

Cómo funciona la integración de Confluence

Confluence es un proveedor de documentación y no un proveedor de código fuente. Tras instalar la aplicación Forge y conectar espacios o páginas en la consola de administración de AWS, AWS Security Agent puede acceder al contenido de Confluence para proporcionar contexto durante las evaluaciones de seguridad.

AWS Security Agent lee el contenido de la página para comprender la arquitectura de la aplicación, los requisitos de seguridad y las decisiones de diseño. Este contexto mejora la calidad y la relevancia

de los hallazgos de seguridad durante las revisiones del diseño, las revisiones del código y las pruebas de penetración.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Un sitio de Confluence Cloud con acceso de administrador
- Una cuenta de Atlassian con privilegios de administrador del sitio
- Permisos para configurar las integraciones en la consola de administración de AWS Security Agent

> **Important**
>
> Un sitio de Atlassian solo se puede asociar a una cuenta de AWS por región. Si necesitas conectar el mismo sitio de Confluence a AWS Security Agent en una cuenta de AWS diferente de la misma región, primero debes eliminar la integración existente.

> **Note**
>
> El precio de la aplicación Atlassian Forge se aplica a esta integración. Para obtener más información, consulta los precios de la plataforma Forge en la documentación de Atlassian.

Registra una conexión de Confluence

1. En la consola de administración de AWS Security Agent, vaya a Integraciones.
2. Seleccione Add Integration.
3. Selecciona Confluence y, a continuación, selecciona Siguiente.
4. Instala la aplicación AWS Security Agent Forge en tu sitio de Atlassian siguiendo las instrucciones que aparecen en pantalla. Tras la instalación, copia el ID de instalación. Consulte the section called “Encuentra tu ID de instalación de Atlassian”.
5. En el campo URL del sitio de Confluence, introduce la URL de tu sitio, por ejemplo`https://acme.atlassian.net`.
6. En el campo ID de instalación, pega el ID de instalación que copiaste de Confluence.
7. Seleccione Autorizar.

Se te redirigirá a Atlassian para autorizar a AWS Security Agent a acceder a tu sitio de Confluence. Una vez completada la autorización, volverás a la consola.

8. En la sección Detalles del registro, introduzca un nombre de registro para esta conexión. Los caracteres válidos son letras, números, puntos, guiones bajos y guiones.
9. Elija Conectar.

Seleccione las páginas de un espacio de agente

Tras registrar la integración de Confluence, conecta páginas específicas a un espacio de agente. Al seleccionar una página, AWS Security Agent obtiene acceso de lectura (recuperación) al contenido de esa página. No hay opciones de funcionalidad por página: el agente lee todas las páginas conectadas. En el paso de revisión del asistente de conexión, puede eliminar las páginas a las que no desee que acceda el agente.

Solucione los problemas de integración de Confluence

Si tienes problemas durante el proceso de integración de Confluence, sigue las siguientes instrucciones para resolver los problemas más comunes.

No se ha podido completar el registro

Si se interrumpe el proceso de registro, es posible que la aplicación Forge esté instalada en tu sitio de Atlassian pero no esté registrada en la consola de AWS.

Resolución

- Regrese a la consola de AWS Security Agent y reinicie el proceso de integración.
- La aplicación Forge permanece instalada y no es necesario volver a instalarla.

La aplicación Forge se ha desinstalado de Atlassian

Si la aplicación AWS Security Agent Forge se desinstala de tu sitio de Atlassian mientras la integración aún existe en AWS Security Agent:

Síntomas

- La integración aparece en la consola de AWS, pero no puede acceder al contenido de Confluence
- Se producen errores al intentar enumerar o leer páginas

Resolución

- Vuelva a instalar la aplicación Forge desde Atlassian Marketplace
- Si el problema persiste, elimine la integración en la consola de AWS y vuelva a registrarla

El sitio ya está conectado a otra cuenta de AWS

Resolución

- Un sitio de Atlassian solo se puede conectar a una cuenta de AWS por región.
- Identifique qué cuenta de AWS tiene la integración existente y úsela o elimine primero la integración existente.

Siguientes pasos

Tras conectar Confluence a AWS Security Agent:

- Diríjase al espacio de agentes en el que desee utilizar esta documentación
- Seleccione páginas específicas para incluirlas como contexto para las revisiones de diseño y las pruebas de penetración
- Cargue documentación adicional a través de S3 si es necesario (consultethe section called “Proporcione recursos a los agentes desde un bucket de S3”)

Eliminar una integración de Confluence

Elimine una integración de Confluence cuando ya no necesite AWS Security Agent para acceder a la documentación de un sitio de Confluence específico.

Requisitos previos para la eliminación

Antes de eliminar una integración de Confluence:

- Comprueba qué Agent Spaces tienen páginas conectadas desde esta integración
- Comprenda el impacto: eliminarla romperá el contexto de la documentación para las revisiones de diseño, las pruebas de penetración y el modelado de amenazas en todos los Agent Spaces que utilicen contenido de esta integración

Paso 1: Eliminar la integración de AWS Security Agent

1. En la consola de administración de AWS Security Agent, vaya a Integraciones.
2. Busca la integración de Confluence que deseas eliminar.
3. Selecciona la integración.
4. Elija Eliminar .
5. Revise el cuadro de diálogo de confirmación y seleccione Confirmar la eliminación.

Paso 2: desinstala la aplicación Forge (opcional)

Tras eliminar la integración de AWS Security Agent, puedes desinstalar opcionalmente la aplicación Forge de tu sitio de Atlassian:

1. En Confluence, dirígete a la administración de Confluence.
2. Selecciona Aplicaciones.
3. Localice Connect with AWS Security Agent.
4. Elija Desinstalar.

Conéctese al control de código fuente alojado de forma privada

> **Important**
>
> Private Connections se encuentra en una versión preliminar de AWS Security Agent y está sujeta a cambios.

AWS Security Agent puede conectarse a sistemas de control de código fuente que se ejecutan en redes privadas, como GitLab Self-Managed instancias y GitHub Enterprise Server. Las conexiones privadas utilizan Amazon VPC Lattice para establecer una conectividad segura entre AWS Security Agent y su infraestructura privada sin exponer sus sistemas a la Internet pública.

Cómo funcionan las conexiones privadas

Una conexión privada crea una ruta de red segura entre AWS Security Agent y un recurso de destino de la VPC. Por fuera, AWS Security Agent utiliza Amazon VPC Lattice para establecer esta

conectividad. VPC Lattice es un servicio de redes de aplicaciones de AWS para conectar, proteger y monitorear el tráfico entre los servicios de las VPC y las cuentas, sin tener que administrar la infraestructura de red subyacente.

Al crear una conexión privada:

1. Usted proporciona la VPC, las subredes y (opcionalmente) los grupos de seguridad que tienen conectividad de red con el servicio de destino.
2. AWS Security Agent crea una puerta de enlace de recursos gestionada por servicios y aprovisiona interfaces de red elásticas (ENI) en las subredes que especificó.
3. El agente usa la puerta de enlace de recursos para enrutar el tráfico a la dirección IP o el nombre DNS del servicio de destino a través de la ruta de red privada.

Service-managed frente a las conexiones privadas autogestionadas

AWS Security Agent admite dos modos de conexiones privadas:

Service-managed(recomendado para configuraciones sencillas):

- AWS Security Agent crea y administra la puerta de enlace de recursos de VPC Lattice por usted.
- El servicio de destino debe ejecutarse en la misma cuenta de AWS en la que se creó el espacio de agentes.
- No puede abarcar varias cuentas de AWS.

Self-managed(para configuraciones avanzadas o multicuentas):

- Usted crea y administra su propia configuración de recursos de VPC Lattice.
- Debe proporcionar el nombre de recurso de Amazon (ARN) de la configuración de recursos existente.
- Admite el acceso entre cuentas (el cliente administra las redes entre cuentas).

Requisitos previos

Antes de crear una conexión privada, compruebe que dispone de:

- Un espacio de agente activo

- Un servicio de destino al que se pueda acceder de forma privada (GitLab Self-Managed o servidor GitHub empresarial) en una dirección IP privada o un nombre DNS conocidos
- El servicio de destino debe atender el tráfico HTTPS con una versión TLS mínima de 1.2
- Subredes en su VPC (de 1 a 20 subredes). Recomendamos seleccionar subredes en varias zonas de disponibilidad para obtener una alta disponibilidad.
- (Opcional) Grupos de seguridad para controlar el tráfico hacia los ENI (hasta 5)

> **Note**
>
> VPC Lattice no admite las siguientes zonas de disponibilidad:`use1-az3`,,,`usw1-az2`,`apne1-az3`, `apne2-az2euc1-az2`,`euw1-az4`. `cac1-az3` `ilc1-az2`

> **Note**
>
> Las conexiones privadas son recursos a nivel de cuenta. Después de crear una conexión privada, puede reutilizarla en varias integraciones y espacios de agentes que necesiten llegar al mismo anfitrión.

> **Note**
>
> Cuando seleccionas una conexión privada para un proveedor que usa la autenticación OAuth, la conexión privada se aplica tanto al punto final del proveedor como al punto final del intercambio de tokens. Asegúrese de que la conexión privada esté configurada con una dirección de host que pueda enrutar el tráfico a ambos puntos finales.

Cree una conexión privada

1. En la consola de administración de AWS Security Agent, vaya a Integraciones.
2. Elija la pestaña Conexiones privadas.
3. Selecciona Crear conexión privada.
4. En Detalles de la conexión, introduce un nombre. Los nombres pueden contener letras minúsculas, números y guiones, y deben empezar y terminar con una letra o un número.

5. En la sección Detalles de conexión, elija cómo se conecta AWS Security Agent a su servicio de destino:
   - Para que AWS Security Agent cree y administre la conexión, deje desactivada la opción Usar la configuración de recursos existente y, a continuación, complete las secciones Ubicación del recurso, Control de acceso y Detalles del objetivo del servicio.
   - Para recorrer una configuración de recursos de VPC Lattice que ya haya creado, seleccione Usar configuración de recursos existente y, a continuación, complete la sección Configuración de recursos existentes. Las secciones gestionadas por el servicio no se aplican.
6. (Service-managed) En la ubicación del recurso:
   a. Seleccione la VPC en la que se encuentra el recurso.
   b. Seleccione una o más subredes. Recomendamos seleccionar subredes en al menos dos zonas de disponibilidad.
   c. (Opcional) Seleccione un tipo de dirección IP (IPv4, IPv6 o pila doble).
7. (Service-managed) En Control de acceso:
   a. Seleccione los grupos de seguridad asociados a los recursos conectados.
   b. (Opcional) En Configuración avanzada, introduzca los rangos de puertos, por ejemplo, hasta 11 puertos o rangos TCP separados por comas. `443, 8080-8090`
8. (Service-managed) En Detalles del objetivo del servicio:
   a. En el campo Dirección del host, introduzca el nombre del host DNS o la dirección IP del servicio de destino.
   b. Para la resolución de DNS, seleccione Pública para una dirección de host que se pueda resolver públicamente o En VPC (DNS privado) para una dirección que solo se pueda resolver dentro de la VPC.
   c. (Opcional) En el campo Clave pública del certificado, introduzca la clave PEM-encoded pública si su destino utiliza un certificado autofirmado o una autoridad de certificación privada. Esto permite que AWS Security Agent confíe en la conexión TLS.
9. (Self-managed) En Configuración de recursos existente, en Configuración de recursos, seleccione una configuración de recursos de VPC Lattice de la lista o introduzca un ID de configuración de recursos (que comience por`rcfg-`) o su ARN. La lista muestra las configuraciones de recursos en la región actual.
10. Elija Crear conexión.

    El estado de la conexión cambia a Crear en curso. Este proceso puede tardar hasta 10 minutos en completarse. Cuando se complete, el estado cambiará a Disponible.

Utilice una conexión privada con una integración

Cuando registre una GitLab Self-Managed integración de GitHub Enterprise Server, seleccione Conectar al punto final mediante una conexión privada y, a continuación, elija su conexión en la lista de conexiones privadas. El agente de seguridad de AWS dirige el tráfico al proveedor a través de esa conexión. En la lista solo aparecen las conexiones con el estado Disponible.

También puedes elegir Crear una conexión privada durante el registro. AWS Security Agent conserva su borrador de registro mientras crea la conexión y, a continuación, lo devuelve al flujo de registro.

Seguridad

- Sin exposición pública a Internet: todo el tráfico permanece en la red de AWS.
- Customer-controlled grupos de seguridad: usted administra las normas de tráfico entrante y saliente.
- Service-linked rol con privilegios mínimos: AWS Security Agent utiliza un rol vinculado a un servicio que se limita a los recursos etiquetados con. `AWSSecurityAgentManaged`

> **Note**
>
> Si su organización tiene políticas de control de servicios (SCP) que restringen las acciones de la API VPC Lattice, la puerta de enlace de recursos gestionados por el servicio se crea mediante un rol vinculado al servicio. Asegúrese de que sus SCP permitan las acciones necesarias para el rol vinculado al servicio.

Verifica una conexión privada

Cuando la conexión privada alcance el estado Disponible, compruebe la conectividad:

- Asegúrese de que el servicio de destino esté funcionando y aceptando conexiones en el puerto esperado
- Compruebe que los grupos de seguridad conectados a los ENI permiten el tráfico saliente en el puerto de destino
- Compruebe que el grupo de seguridad de su servicio permita el tráfico entrante desde las IP del plano de datos de VPC Lattice dentro del rango CIDR de su VPC

- Confirme que las tablas de enrutamiento de subredes permiten el tráfico entre las subredes de ENI y su servicio

Elimine una conexión privada

1. En la consola de AWS Security Agent, vaya a Integraciones.
2. Elija la pestaña Conexiones privadas.
3. Selecciona la conexión privada que deseas eliminar.
4. Elija Eliminar.

> **Important**
>
> No puedes eliminar una conexión privada que esté siendo utilizada actualmente por una integración. Elimine primero la integración y, a continuación, elimine la conexión privada.

Siguientes pasos

- the section called “Conecta AWS Security Agent a GitLab Self-Managed”- Conectar una GitLab instancia privada
- the section called “Connect AWS Security Agent a un servidor GitHub empresarial”- Conectar un servidor GitHub empresarial privado

Conectar el agente a los recursos de VPC privados

Si la aplicación en la que desea ejecutar una prueba de penetración no está disponible en la Internet pública, debe proporcionar a AWS Security Agent una configuración de VPC. AWS Security Agent utilizará esta configuración de VPC, que incluye una VPC, una subred y grupos de seguridad, para acceder a la aplicación.

> **Note**
>
> Al probar los puntos finales en una VPC privada, solo se permiten los puntos finales que se resuelvan en IP de rangos de IP privadas conocidas (consulte Bloques CIDR de VPC para obtener más información). Se permiten los siguientes rangos de IPv4 e IPv6:

```
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
fd00::/8
```

> **Note**
>
> Al conectarse a una subred, AWS Security Agent creará una ENI (interfaz de red elástica) en la subred configurada para la prueba de penetración. Este ENI no tiene una dirección IP pública asociada, lo que significa que no puede comunicarse con las pasarelas de Internet de VPC en las subredes públicas. Si su prueba de penetración requiere acceso abierto a Internet, utilice una subred privada con una puerta de enlace NAT de VPC asociada en su lugar.

Usted concede a AWS Security Agent acceso general a una VPC desde la consola de administración de AWS. En la aplicación web Security Agent, los usuarios seleccionan la configuración específica para una prueba de penetración.

Para añadir una VPC en el espacio de agentes

1. Navegue a la página de información general del espacio de agentes
2. Seleccione Acciones y, a continuación, Editar la configuración de la prueba de penetración
3. En el encabezado VPC, especifique la VPC, las subredes y los grupos de seguridad.

Puede añadir hasta 5 VPC.

Permisos de rol de agente, espacio y servicio necesarios.

Para ejecutar una prueba de penetración con una VPC, su rol de servicio de espacio de agente debe incluir los siguientes permisos:

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

```
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateNetworkInterfacePermission",
      "Resource": "arn:aws:ec2:{{region}}:{{accountId}}:network-interface/*",
      "Condition": {
        "ArnEquals": {
          "ec2:Subnet": [
            "arn:aws:ec2:{{region}}:{{accountId}}:subnet/[[subnetIds]]"
          ]
        }
      }
    }
  ]
}
```

Para seleccionar una configuración de VPC específica para una prueba de penetración en la aplicación web Security Agent

1. Diríjase a la página de información general sobre las pruebas de penetración
2. Seleccione la prueba de penetración para la que necesita agregar la configuración de VPC y, a continuación, elija Modificar los detalles de la prueba de penetración.
3. Seleccione Siguiente para acceder a la sección de recursos de VPC.
4. Seleccione los grupos de VPC, subred y seguridad
5. Seleccione Siguiente para ir a la última sección y guardar la prueba de penetración

> **Note**
>
> Cross-account Actualmente, se admiten las pruebas de penetración para los recursos de VPC (subredes y grupos de seguridad) compartidos mediante AWS Resource Access Manager. Los secretos de Secrets Manager y las funciones de Lambda que se utilizan para las credenciales de autenticación deben configurarse en la misma cuenta de AWS que la configuración de AWS Security Agent.

Ejecutar una prueba de penetración con recursos de VPC en otra cuenta de AWS

Puede ejecutar pruebas de penetración en los recursos de VPC compartidos con su cuenta mediante AWS Resource Access Manager. Ambas cuentas deben formar parte de la misma organización de AWS.

1. (Opcional) Habilite el uso compartido automático de recursos para su organización de AWS

```
aws ram enable-sharing-with-aws-organization
```

2. Con las credenciales de la cuenta de AWS propietaria de los recursos de la VPC, comparta los recursos de la subred y del grupo de seguridad con la cuenta del propietario de la prueba de penetración

```
aws ram create-resource-share \
    --name SharePentestResources \
    --resource-arns <subnet ARN> <security group ARN> \
    --principals <penetration test owner account ID>
```

3. Diríjase a la página de información general de Agent Space
4. Seleccione Prueba de penetración y busque el nombre del rol de servicio
5. Compruebe que la función de IAM concede acceso a los recursos de VPC compartidos.
6. Seleccione Acciones y, a continuación, Editar la configuración de la prueba de penetración
7. En el encabezado VPC, especifique la VPC, las subredes y los grupos de seguridad compartidos y guarde la configuración actualizada.

8. Vaya a la página de información general sobre las pruebas de penetración en la aplicación web AWS Security Agent.
9. Seleccione la prueba de penetración para la que necesita agregar la configuración de VPC y, a continuación, elija Modificar los detalles de la prueba de penetración.
10. Actualice la prueba de penetración para usar los recursos de VPC compartidos

Configurar capacidades

Habilite y configure las pruebas de penetración, la revisión del código y el modelado de amenazas para sus Agent Spaces, incluidas las soluciones, las fuentes de S3 y los dominios de destino.

Habilitar la prueba de penetración

Configure AWS Security Agent para ejecutar pruebas de penetración autónomas en sus aplicaciones. Esta configuración permite a AWS Security Agent acceder a sus recursos de AWS, verificar la propiedad del dominio y realizar pruebas de seguridad exhaustivas que identifican las vulnerabilidades explotables en sus aplicaciones web y API.

Al habilitar las pruebas de penetración, AWS Security Agent puede validar de forma continua la seguridad de las aplicaciones sin las demoras de las pruebas manuales. Al configurar las integraciones de AWS necesarias, se asegura de que AWS Security Agent pueda probar aplicaciones públicas y privadas, registrar los resultados y acceder a CloudWatch las credenciales para las pruebas autenticadas.

En este procedimiento, configurará los dominios de destino, configurará opcionalmente las funciones de VPC, CloudWatch registro, almacenamiento de credenciales y Lambda para realizar pruebas, configurará las integraciones de S3 para proporcionar contexto adicional y configurará el acceso a los servicios mediante funciones de IAM.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Cuenta de AWS con permisos administrativos para crear funciones de IAM
- Capacidad de verificación de la propiedad del dominio (modificación de registros DNS o HTTP)
- Seleccione dominios o aplicaciones para probarlos
- Detalles de configuración de VPC (opcional) si se prueban aplicaciones privadas

- (Opcional) Depósito S3 si proporciona artefactos adicionales a AWS Security Agent

Paso 1: Configurar el dominio

En el primer paso del asistente, especifique los dominios de destino que quiere probar y cómo AWS Security Agent debe verificar la propiedad.

1. En la sección Dominios de destino, introduzca su dominio en el campo Dominio.
2. Selecciona un método de verificación:
   - DNS_TXT: demuestre la propiedad del dominio añadiendo un registro TXT a la configuración de DNS de su dominio.
   - HTTP_ROUTE: demuestra la propiedad del dominio alojando un archivo de verificación en una URL específica de tu dominio.
   - PRIVATE_VPC: solo se puede utilizar para pruebas de penetración de VPC privadas. Comprueba que el dominio se resuelve en una IP de un rango de CIDR privado
   - Para obtener más información, consulte the section called “Habilitar un dominio de aplicación para las pruebas de penetración”.
3. Seleccione Añadir otro dominio para añadir dominios adicionales (hasta 5 en total).
4. Selecciona Siguiente para proceder a la verificación del dominio.

Paso 2: Verificar los dominios

En el segundo paso del asistente, compruebe la propiedad de cada dominio que haya configurado. AWS Security Agent requiere una propiedad verificada antes de poder realizar las pruebas de penetración.

1. Revise los dominios que aparecen en la tabla de dominios de destino.
2. Para cada dominio, selecciónelo y active la verificación según el método que haya elegido:
   - Dominios de Route 53 (la misma cuenta de AWS): elige la One-click verificación. AWS Security Agent crea automáticamente el registro DNS y completa la verificación.
   - DNS TXT (otros proveedores de DNS): copie el token de verificación, añada el registro TXT a su registrador de DNS y, a continuación, seleccione el dominio y elija Verificar.
   - Ruta HTTP: coloca el token de verificación en la ruta requerida de tu servidor web, selecciona el dominio y elige Verificar. Para obtener más información, consulte the section called “Habilitar un dominio de aplicación para las pruebas de penetración”.

3. Selecciona Siguiente para continuar con la configuración opcional.

> **Note**
>
> Sub-domains de un dominio verificado no requieren una verificación individual cuando se utiliza la verificación de ruta DNS, TXT o HTTP. Para la verificación de la VPC privada, el nombre del dominio del punto final de destino debe coincidir con el nombre de dominio completo configurado para la verificación.

> **Note**
>
> En el caso de los dominios privados dentro de una VPC, puede continuar incluso si el estado de verificación del dominio es INALCANZABLE. AWS Security Agent intentará verificar el dominio de los puntos de enlace privados al comienzo de cada pentest.

Paso 3: (opcional) Configurar capacidades adicionales

El tercer paso del asistente le permite configurar los recursos opcionales de AWS para ampliar el alcance de las pruebas de penetración. Todas las secciones de este paso son opcionales y están comprimidas de forma predeterminada.

(Opcional) Configurar los ajustes de la VPC

Si planea probar dominios de destino privados alojados en una VPC, configure los ajustes de VPC para AWS Security Agent. Esta sección es opcional y está comprimida de forma predeterminada.

1. Amplíe la sección de VPC.
2. En el menú desplegable VPC, selecciona la VPC que aloja tus dominios de destino privados.
3. En el menú desplegable Subred, selecciona las subredes de VPC que AWS Security Agent debe usar:

> **Tip**
>
> Para obtener una alta disponibilidad, seleccione varias subredes de varias zonas de disponibilidad. Asegúrese de que sus subredes incluyan una puerta de enlace NAT para la conectividad saliente.

4. En el menú desplegable de grupos de seguridad, seleccione los grupos de seguridad de VPC que AWS Security Agent debe usar:

> **Important**
>
> Asegúrese de que sus grupos de seguridad permitan las conexiones salientes para que AWS Security Agent realice las pruebas de penetración.

(Opcional) Configure CloudWatch el registro

Configure CloudWatch para almacenar los registros de las pruebas de penetración realizadas. Esta sección es opcional y está comprimida de forma predeterminada.

1. Amplíe la sección de CloudWatch registros.
2. En el menú desplegable Grupos de registros, selecciona los grupos de CloudWatch registros existentes
3. Si no selecciona ningún grupo de registros, AWS Security Agent creará un grupo de registros denominado `/aws/securityagent/<agent name>/<pentest id>` con los permisos adecuados.

> **Note**
>
> Asegúrese de que su función de IAM tenga permisos para escribir en el grupo de CloudWatch registros seleccionado.

(Opcional) Configure los secretos de las credenciales de prueba

Si su aplicación requiere credenciales de autenticación para las pruebas, AWS Security Agent puede recuperarlas de forma segura de AWS Secrets Manager. Esta sección es opcional y está comprimida de forma predeterminada.

1. Amplíe la sección Secretos.
2. Seleccione los secretos de AWS Secrets Manager que contienen las credenciales de su aplicación.
3. Al configurar una prueba de penetración en la aplicación web, puede hacer referencia a estos secretos para realizar pruebas autenticadas.

> **Important**
>
> Las credenciales se cifran y almacenan en AWS Secrets Manager. Asegúrese de que su función de IAM tenga permisos para acceder a Secrets Manager para que AWS Security Agent utilice estas credenciales durante las pruebas.

(Opcional) Configurar las funciones de Lambda para las credenciales de prueba

Configure las funciones de Lambda que puedan proporcionar credenciales a su aplicación durante las pruebas. Esta sección es opcional y está comprimida de forma predeterminada.

1. Amplíe la sección de funciones Lambda.
2. Seleccione las funciones Lambda que pueden proporcionar credenciales de autenticación para su aplicación.
3. AWS Security Agent invocará estas funciones durante las pruebas de penetración para obtener credenciales de forma dinámica.

> **Note**
>
> Asegúrese de que su función de IAM tenga permisos para invocar las funciones de Lambda especificadas. Las funciones Lambda deben devolver las credenciales en el formato esperado para que AWS Security Agent las utilice durante las pruebas.

(Opcional) Configure el bucket de S3

Proporcione los detalles del bucket de S3 si planea cargar documentos o artefactos para proporcionarlos como entrada a AWS Security Agent. Esta sección es opcional y está comprimida de forma predeterminada.

1. Amplíe la sección de cubos S3.
2. En el campo Bucket, introduce o busca el nombre de tu bucket de S3.

> **Note**
>
> También puede conectar GitHub los repositorios más adelante o cargar archivos directamente en la aplicación web. La información proporcionada puede garantizar una cobertura exhaustiva, reducir los falsos positivos y ofrecer resultados procesables.

(Opcional) Configure el acceso al servicio

AWS Security Agent requiere un rol de IAM para acceder a sus recursos de AWS (VPC CloudWatch , grupos de registros, Secrets Manager, funciones de Lambda, etc.) para realizar pruebas de penetración. Esta sección es opcional y está comprimida de forma predeterminada.

1. Amplíe la sección de acceso al servicio.
2. De forma predeterminada, AWS Security Agent utiliza un rol de IAM predeterminado con los permisos necesarios para las pruebas de penetración.
3. Para personalizar el rol de IAM, seleccione una de las siguientes opciones:
   a. Crear rol predeterminado: AWS Security Agent crea automáticamente un nuevo rol de IAM con los permisos necesarios
   b. Utilice un rol de servicio existente: seleccione un rol de IAM existente en el menú desplegable
4. Si utiliza un rol existente:
   a. Selecciona el menú desplegable en Elige un rol existente
   b. Seleccione su función de IAM de la lista
   c. Elija el icono de actualización para actualizar la lista si es necesario

> **Note**
>
> La función de IAM predeterminada incluye permisos para acceder a los recursos de la VPC, los grupos de registros CloudWatch , Secrets Manager, las funciones de Lambda y otros servicios necesarios para las pruebas de penetración. Se recomienda utilizar la función de IAM predeterminada, a menos que tenga requisitos de seguridad específicos.

Paso 4: Guarde y active las pruebas de penetración

Tras configurar todos los ajustes necesarios, active las pruebas de penetración para su agente de AWS Security Agent.

1. Revise todas las secciones de configuración para garantizar su precisión.
2. Seleccione Save.
3. AWS Security Agent valida la configuración y crea los recursos de AWS necesarios.

Siguientes pasos

Tras habilitar las pruebas de penetración:

- Configure los alcances de las pruebas de penetración en la aplicación web AWS Security Agent
- Configure las preferencias de notificación para los resultados de las pruebas
- Revise y responda a los resultados de las pruebas de penetración a medida que se vayan descubriendo
- (Opcional) Configure repositorios adicionales para corregir los hallazgos

Para obtener más información sobre la ejecución y la administración de las pruebas de penetración, consulte la documentación de la aplicación web AWS Security Agent.

Habilitar la revisión del código de las solicitudes de extracción para los GitHub repositorios

La revisión del código de la solicitud de extracción ahora está configurada como parte del asistente de configuración de la revisión del código. Al conectar GitHub los repositorios a su espacio de agente, puede habilitar los comentarios de las solicitudes de extracción para los repositorios

individuales para que AWS Security Agent analice automáticamente las solicitudes de extracción y publique los hallazgos de seguridad.

Para obtener instrucciones de configuración completas, consulte. the section called “Habilitar la revisión de código”

Para obtener información sobre cómo aparecen los resultados de las solicitudes de extracción GitHub y cómo responder a ellos, consultathe section called “Revisa los hallazgos de seguridad del código en las solicitudes de cambios”.

Habilitar la revisión de código

Configure su espacio de agente para permitir la revisión del código conectando el código fuente desde GitHub repositorios o buckets de S3. La revisión del código analiza su código fuente para detectar vulnerabilidades de seguridad y cumplir con los requisitos de seguridad personalizados de su organización.

Configurar las configuraciones de revisión de código es una Space-wide operación del agente. Las integraciones y los buckets de S3 que conecte se comparten en todas las capacidades, incluidas la revisión del código y las pruebas de penetración.

Tras completar la configuración, los usuarios pueden crear y ejecutar revisiones de código en la aplicación web AWS Security Agent para analizar los repositorios y las fuentes de S3 en busca de problemas de seguridad.

> **Note**
>
> Si ya tiene GitHub repositorios conectados a su espacio de agente (por ejemplo, mediante una configuración de pruebas de penetración), la revisión del código ya está habilitada. Puede omitir esta configuración e ir directamente a la aplicación web para crear revisiones de código. Consulte the section called “Crear una revisión de código”.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Un espacio de agente creado en la consola de administración de AWS (consultethe section called “Crear un espacio de agentes”)

- Al menos una de las siguientes entradas de código fuente:
  - Una cuenta de usuario o GitHub organización con la GitHub aplicación AWS Security Agent instalada (consultethe section called “Connect AWS Security Agent a los GitHub repositorios”)
  - Un bucket de S3 que contiene el código fuente que desea revisar
- Permisos para configurar las integraciones de su espacio de agente
- (Opcional) Habilite al menos un requisito de seguridad en un paquete de requisitos de seguridad si planea utilizar la validación de requisitos de seguridad (consultethe section called “Gestione los requisitos de seguridad”)

Acceda al asistente de configuración de revisión de código

Navegue hasta la configuración de revisión de código de su espacio de agente.

1. En la consola de AWS Security Agent, seleccione su espacio de agente.
2. Elija Habilitar la revisión del código en una de las siguientes ubicaciones:
   - La tarjeta de revisión del código
   - En la pestaña Revisión de código, selecciona Habilitar revisión de código

> **Tip**
>
> Si desea que AWS Security Agent aborde automáticamente los comentarios sobre la revisión del código, active también la corrección del código. Para obtener más información, consulte the section called “Permita a los usuarios iniciar la corrección de los hallazgos de las pruebas de penetración y la revisión del código”.

Se le dirigirá al asistente de configuración para revisar el código de configuración.

Paso 1: Conectar integraciones, repositorios y depósitos

En el primer paso del asistente, conecte las entradas de código fuente y configure los ajustes de revisión de código. Debe añadir al menos un GitHub repositorio o depósito de S3 para continuar.

> **Important**
>
> Las integraciones y los depósitos de S3 configurados aquí se comparten en su espacio de agente. Los cambios se aplican tanto a las capacidades de revisión del código como a las pruebas de penetración.

Connect GitHub repositorios

Añada GitHub repositorios de sus GitHub organizaciones o cuentas de usuario autorizadas. Si selecciona Añadir, se abre el GitHub asistente Connect de dos pasos, en el que primero selecciona los repositorios y, a continuación, configura las acciones que AWS Security Agent puede realizar en cada uno de ellos.

1. En la sección Integraciones conectadas, elija Agregar.
2. Seleccione el GitHub registro que contiene los repositorios que desea revisar.
3. En el paso Conectar GitHub repositorios, selecciona la casilla de verificación de cada repositorio al que quieras conectar.
4. Selecciona Siguiente para ir a Administrar las capacidades.

> **Note**
>
> Se accede a los repositorios conectados en modo de solo lectura para analizar el código durante la revisión del código y las pruebas de penetración. En el siguiente paso, debes configurar las acciones de escritura, como publicar comentarios de revisión y abrir solicitudes de corrección.

> **Note**
>
> Si aún no ha registrado una GitHub integración, elija Configuración para ir a la página de integraciones, donde podrá autorizar la GitHub aplicación AWS Security Agent. Para obtener más información, consulte the section called “Connect AWS Security Agent a los GitHub repositorios”.

Configure las capacidades GitHub del repositorio

En el paso Administrar capacidades del GitHub asistente Connect, elija lo que AWS Security Agent puede hacer en cada repositorio. Los comentarios de revisión del código y la corrección del código se configuran de forma independiente en cada repositorio.

1. Para cada repositorio, active los comentarios de revisión de código para que AWS Security Agent publique los hallazgos de seguridad como comentarios en las solicitudes de incorporación de cambios.
2. Para cada repositorio, active la corrección de código para permitir que AWS Security Agent corrija los hallazgos. Cuando está habilitada, los usuarios de aplicaciones web pueden solicitar solicitudes de extracción que corrijan los hallazgos, y los autores de las solicitudes de extracción pueden hacer comentarios `@AWS-Security-Agent fix all findings.` para que el agente aborde sus comentarios de revisión.
3. Selecciona Guardar para aplicar tus selecciones y volver al asistente de configuración de la revisión del código.

Cuando los comentarios de revisión de código están habilitados para un repositorio:

- AWS Security Agent analiza automáticamente las solicitudes de cambios cuando están marcadas como «Listas para revisión». Los borradores de solicitudes de extracción no se analizan.
- Los hallazgos de seguridad se publican como comentarios de revisión directamente en la solicitud de cambios, junto con una guía de corrección específica.
- El análisis utiliza los ajustes de revisión de código configurados (vulnerabilidades de seguridad, requisitos personalizados o ambos).

> **Note**
>
> Los comentarios de las solicitudes de extracción solo están disponibles para los GitHub repositorios privados.

Cuando la corrección de código está habilitada para un repositorio, los usuarios de aplicaciones web pueden iniciar la corrección de los resultados de la revisión del código y de las pruebas de penetración en ese repositorio, y AWS Security Agent entrega cada corrección como una solicitud de

extracción. Para obtener más información, consulte the section called “Permita a los usuarios iniciar la corrección de los hallazgos de las pruebas de penetración y la revisión del código”.

Para obtener más información sobre cómo aparecen los resultados de las solicitudes de extracción GitHub y cómo responder a ellos, consulta. the section called “Revisa los hallazgos de seguridad del código en las solicitudes de cambios”

Agrega cubos S3

Agregue depósitos S3 que contengan código fuente o recursos contextuales para revisar el código.

1. En la sección de cubos de S3, selecciona Añadir recurso de S3.
2. Introduce el URI de S3 para el bucket o el prefijo que contiene tu código fuente.
3. Elija Añadir.

> **Note**
>
> Puede añadir hasta 10 recursos de S3. Los cubos de S3 se comparten entre las distintas capacidades, incluidas la revisión del código y las pruebas de penetración.

> **Tip**
>
> Puede añadir buckets de S3 que contengan código fuente, archivos de configuración, plantillas de infraestructura como código u otros artefactos que desee que AWS Security Agent analice para detectar problemas de seguridad.

Configure los ajustes de revisión de código

Configure los tipos de problemas de seguridad que AWS Security Agent analiza durante las revisiones del código. Esta configuración se aplica a todos los repositorios y fuentes con la revisión de código habilitada en este espacio de agentes.

1. En la sección de configuración de revisión de código, selecciona una de las siguientes opciones:
   - Validación de los requisitos de seguridad: valide si el código cumple con los requisitos de seguridad que ha habilitado en sus paquetes de requisitos de seguridad.

- Hallazgos sobre vulnerabilidades de seguridad: identifique las vulnerabilidades de seguridad más comunes en el código.
- Requisitos de seguridad y hallazgos de vulnerabilidades: analice el código para comprobar si cumple con los requisitos de seguridad que ha activado y si presenta las vulnerabilidades de seguridad más comunes. Esta es la configuración predeterminada.

> **Note**
>
> Cuando la validación de requisitos de seguridad está habilitada, AWS Security Agent compara el código con los requisitos de seguridad que haya habilitado en sus paquetes de requisitos de seguridad. Si selecciona la validación de los requisitos de seguridad pero no tiene al menos un requisito de seguridad activado, AWS Security Agent no identificará los resultados basados en los requisitos. Para obtener más información sobre los requisitos de seguridad, consulte the section called “Gestione los requisitos de seguridad”.

1. Seleccione Siguiente para continuar con las configuraciones opcionales.

Paso 2: Configuraciones opcionales

En el segundo paso del asistente, configure los ajustes opcionales de CloudWatch registro y acceso a los servicios para su entorno de revisión de código.

(Opcional) Configure CloudWatch los registros

Configure grupos de CloudWatch registros para capturar y analizar el comportamiento de las aplicaciones durante la revisión del código.

1. Amplíe la sección de CloudWatch registros.
2. En el menú desplegable Grupos de registros, seleccione uno o más grupos de CloudWatch registros existentes de su cuenta de AWS.

> **Note**
>
> Si no selecciona un grupo de registros, AWS Security Agent crea automáticamente un grupo de registros predeterminado para almacenar los registros de ejecución de revisiones de código.

(Opcional) Configure el acceso al servicio

Configure la función de servicio de IAM que el agente de seguridad de AWS utiliza para acceder a sus recursos de AWS, como los buckets y los CloudWatch registros de S3, para revisar el código.

1. Amplíe la sección de acceso al servicio.
2. Seleccione una de las siguientes opciones:
   - Crear rol predeterminado: AWS Security Agent crea automáticamente un nuevo rol de IAM con los permisos necesarios para revisar el código.
   - Utilice un rol de servicio existente: seleccione un rol de IAM existente en el menú desplegable.
3. Si utiliza el rol predeterminado, introduzca un nombre para el rol de servicio. El nombre debe ser único en todos los roles de la cuenta, usar caracteres alfanuméricos y `+=,.@-_` caracteres y no puede incluir espacios.

> **Note**
>
> El nombre del rol de servicio tiene una longitud máxima de 64 caracteres. Si no selecciona un rol existente, se crea automáticamente un rol de servicio.

1. Elija Guardar para completar la configuración.

Después de la configuración

Tras completar el asistente de configuración de revisión del código:

- La tarjeta de revisión del código de la página de Agent Space muestra el estado Listo.
- Los usuarios pueden iniciar la aplicación web y crear revisiones de código para escanear los repositorios conectados y las fuentes de S3.

- Puede modificar su configuración en cualquier momento seleccionando Editar configuración en la pestaña Revisión de código.

Edite la configuración de revisión del código

Para modificar la configuración de revisión de código después de la configuración inicial:

1. Diríjase a su espacio de agente en la consola de AWS Security Agent.
2. Seleccione la pestaña Revisión de código.
3. Elija Editas configuración.
4. Actualice las integraciones, los depósitos de S3, la configuración de revisión de código, CloudWatch los registros o el acceso a los servicios según sea necesario.
5. Seleccione Save.

Siguientes pasos

Después de configurar las configuraciones de revisión del código:

- Inicie la aplicación web para crear y ejecutar revisiones de código (consultethe section called “Crear una revisión de código”)
- Conecta GitHub repositorios adicionales o depósitos de S3 a medida que crece tu base de código
- Configure los paquetes de requisitos de seguridad para la validación específica de la organización (consulte) the section called “Gestione los requisitos de seguridad”
- Revisa cómo aparecen los resultados de las solicitudes de extracción en GitHub (consulte) the section called “Revisa los hallazgos de seguridad del código en las solicitudes de cambios”

Habilitar el modelado de amenazas

Configure su espacio de agente para permitir el modelado de amenazas conectando los repositorios de código fuente y configurando los recursos de AWS. El modelado de amenazas analiza la arquitectura de su aplicación e identifica las amenazas de seguridad a partir del código fuente, los documentos de diseño o ambos.

La configuración del modelado de amenazas es una Space-wide operación del agente. Las integraciones y los buckets de S3 que conecte se comparten en todas las capacidades, como el modelado de amenazas, la revisión del código y las pruebas de penetración.

Tras completar la configuración, los usuarios pueden crear y ejecutar modelos de amenazas en la aplicación web AWS Security Agent.

> **Note**
>
> Si ya tiene repositorios o depósitos de S3 conectados a su espacio de agente (por ejemplo, mediante una revisión del código o una configuración de pruebas de penetración), es posible que el modelado de amenazas ya esté habilitado. Puede ir directamente a la aplicación web para crear un modelo de amenazas. Consulte the section called “Cree un modelo de amenazas”.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Un espacio de agente creado en la consola de administración de AWS (consultethe section called “Crear un espacio de agentes”)
- Permisos para configurar las integraciones de su espacio de agente
- (Opcional) Una GitHub organización o Bitbucket con la aplicación AWS Security Agent instalada (consulte Conectar el agente de seguridad de AWS a los repositorios, Conectar el agente de seguridad de AWS a GitHub los repositorios o Conectar el agente de seguridad de AWS a GitLab los repositorios de Bitbucket) GitLab

Acceda al asistente de configuración del modelado de amenazas

Navegue hasta la configuración de modelado de amenazas de su espacio de agente.

1. En la consola de AWS Security Agent, seleccione su espacio de agente.
2. Elija Configurar el modelo de amenazas en la tarjeta del modelo de amenazas o en la pestaña Modelo de amenazas.

Se le dirigirá al asistente para configurar el modelo de amenazas, que consta de dos pasos opcionales.

Paso 1: Conectar los repositorios de código fuente (opcional)

Conecta los GitHub repositorios de Bitbucket o Bitbucket para los que quieras habilitar el modelado de amenazas. GitLab Los propios modelos de amenazas se crean y visualizan en la aplicación web.

> **Important**
>
> Las integraciones configuradas aquí se comparten en todo su espacio de agente. Los cambios se aplican a las capacidades de modelado de amenazas, revisión de código y pruebas de penetración.

Connect repositorios

1. En la sección Integraciones conectadas, selecciona Agregar.
2. Seleccione el registro que contiene los repositorios que quiere usar.
3. Seleccione la casilla de verificación de cada repositorio al que desee conectarse.
4. Elija Guardar para aplicar las selecciones.

> **Note**
>
> Si aún no ha registrado una integración, elija Configuración para ir a la página de integraciones, donde podrá autorizar la aplicación AWS Security Agent. Para obtener más información, consulte Conectar el agente de seguridad de AWS a GitHub los repositorios, Conectar el agente de seguridad de AWS a GitLab los repositorios o Conectar el agente de seguridad de AWS a los repositorios de Bitbucket.

1. Seleccione Siguiente para continuar con las configuraciones opcionales.

Paso 2: Configuraciones opcionales

Configure los ajustes de acceso a los servicios, los CloudWatch registros y los depósitos de S3 para su entorno de modelado de amenazas. Estos ajustes se comparten con otras funciones de su espacio de agente.

Depósitos S3 (opcionales)

Añada depósitos S3 que contengan el código fuente que desee que el agente utilice como contexto durante el modelado de amenazas.

1. En la sección de cubos de S3, elija Agregar recurso de S3.
2. Introduce el URI de S3 para el depósito o el prefijo.
3. Elija Añadir.

> **Note**
>
> Puede añadir hasta 10 recursos de S3.

CloudWatch registros (opcional)

Configure grupos de CloudWatch registros para capturar y analizar el comportamiento de las aplicaciones durante la ejecución del modelo de amenazas.

1. En la sección de CloudWatch registros, seleccione uno o más grupos de CloudWatch registros existentes de su cuenta de AWS.

Acceso a los servicios

Configure la función de servicio de IAM que AWS Security Agent utiliza para acceder a sus recursos de AWS, como los buckets y los CloudWatch registros de S3, para modelar las amenazas. Se requiere un rol de servicio para permitir el modelado de amenazas.

1. En la sección Acceso al servicio, seleccione un rol de servicio de IAM existente en el menú desplegable o déjelo vacío para que se cree automáticamente un rol de servicio.

> **Note**
>
> Si no selecciona una función existente, se creará automáticamente una función de servicio.

1. Elija Guardar para completar la configuración.

Después de la configuración

Tras completar la configuración del modelado de amenazas:

- La tarjeta del modelo de amenazas de la página de Agent Space muestra el estado Listo.
- Los usuarios pueden iniciar la aplicación web y crear modelos de amenazas a partir del código fuente conectado, los documentos de alcance subidos, las páginas de Confluence o una combinación de estas entradas.

Siguientes pasos

Tras habilitar el modelado de amenazas:

- Inicie la aplicación web para crear y ejecutar modelos de amenazas (consulte Crear un modelo de amenazas)
- Conecta repositorios adicionales o depósitos de S3 a medida que crece tu base de código
- Conecta Confluence para permitir la selección de páginas como documentos de alcance (consulta Conectar AWS Security Agent a Confluence)

Permita a los usuarios iniciar la corrección de los hallazgos de las pruebas de penetración y la revisión del código

En la consola de administración de AWS, puede habilitar la corrección automática para que los usuarios de la aplicación web AWS Security Agent puedan solicitar correcciones para un hallazgo específico. AWS Security Agent entrega cada corrección como una solicitud de GitHub extracción en el repositorio afectado.

Puede habilitar la corrección por repositorio desde un espacio de agentes. Las pestañas Prueba de penetración y Revisión de código abren el mismo asistente de configuración del repositorio, por lo que puede utilizar cualquiera de las pestañas para gestionar la configuración habilitada para la corrección automática. La corrección se aplica a los hallazgos de ambas capacidades, por lo que solo necesita habilitarla una vez por repositorio.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

1. Se habilitaron las pruebas de penetración (consultethe section called “Habilitar la prueba de penetración”) o la revisión del código (consultethe section called “Habilitar la revisión de código”)
2. Instalación y autorización de la GitHub aplicación AWS Security Agent para su GitHub organización (consultethe section called “Connect AWS Security Agent a los GitHub repositorios”)

Abra el asistente de configuración del repositorio

Elija el punto de entrada que coincida con la configuración de sus repositorios.

Desde la pestaña Prueba de penetración

Utilice esta ruta para añadir GitHub repositorios para las pruebas de penetración y configurar la corrección en la misma pasada.

1. Navegue a la página de información general de Agent Space.
2. Seleccione la pestaña Prueba de penetración.
3. Selecciona un GitHub registro que sea propietario de tus repositorios:
   a. Si no ha asociado ningún GitHub registro al espacio de agentes, seleccione Añadir en el cuadro de información de Connect GitHub to AWS Security Agent para seleccionar un registro.
   b. Si ya hay uno o más GitHub registros asociados, seleccione Añadir en la sección Integraciones conectadas para seleccionar otro.
4. Seleccione Siguiente para elegir GitHub los repositorios.
5. Elija Siguiente para configurar las capacidades del repositorio.

Desde la pestaña de revisión de código

Usa esta ruta cuando tus repositorios ya estén conectados para revisar el código.

1. Navegue a la página de información general de Agent Space.
2. Seleccione la pestaña de revisión de código.
3. En la tabla de GitHub repositorios, seleccione Editar para abrir el asistente de configuración del repositorio.

Active la corrección automática y guarde

Cuando llegue a las capacidades del repositorio, siga cualquiera de las rutas anteriores:

1. En la columna Habilitación de la corrección automática, marque como Habilitada cada repositorio que desee corregir.
2. Seleccione Connect para guardar la configuración.

Los usuarios de la aplicación web ahora pueden iniciar la corrección de los hallazgos en estos repositorios, y AWS Security Agent abrirá solicitudes de cambios con las correcciones propuestas.

Proporcione recursos a los agentes desde un bucket de S3

Puede conceder a AWS Security Agent acceso a los recursos de un bucket de S3, como documentos de API, documentos de modelos de amenazas y código fuente que respaldan las pruebas de penetración.

Usted concede a AWS Security Agent acceso de lectura a un bucket de S3 en la consola de administración de AWS. En la aplicación web Security Agent, los usuarios seleccionan los recursos individuales de S3 según corresponda.

1. Diríjase a la página de información general de Agent Space
2. Seleccione Acciones y, a continuación, Editar la configuración de la prueba de penetración
3. En la sección de cubos de S3, defina el URI de S3 que contiene el depósito de S3. Puede añadir varios depósitos de S3.

Habilitar un dominio de aplicación para las pruebas de penetración

Antes de poder ejecutar una prueba de penetración en una aplicación, debe agregar un dominio de destino y verificar su propiedad. AWS Security Agent solo realizará pruebas de penetración en dominios verificados.

> **Note**
>
> No necesita validar los dominios auxiliares que pueda utilizar su aplicación. Solo necesita validar el dominio con el que realizará activamente las pruebas de penetración.

Paso 1: Agrega un dominio de destino

Para añadir un dominio de destino, vaya a la pestaña Prueba de penetración en la página de información general de Agent Space. En función de si ya ha configurado las pruebas de penetración, utilice uno de los siguientes métodos:

- First-time configuración: seleccione Configurar prueba de penetración para abrir el asistente de pruebas de penetración. En el primer paso, introduce el dominio y elige un método de verificación.
- Añadir un dominio a una configuración existente: en la tabla Dominios de destino, seleccione Añadir dominio. Introduzca el dominio y elija un método de verificación en el modal.

Puedes añadir un dominio base o un subdominio, como `example.com` o`billing.example.com`. AWS sugiere usar un subdominio en el que tenga permiso para crear `TXT` registros.

> **Note**
>
> Cuando verifica un dominio mediante la verificación de ruta DNS, TXT o HTTP, los subdominios de ese dominio quedan cubiertos automáticamente. Por ejemplo, la verificación te `example.com` permite realizar pruebas `api.example.com` o `billing.example.com` sin verificación adicional. Para la verificación de la VPC privada, el nombre del dominio del punto final de destino debe coincidir con el nombre de dominio completo configurado para la verificación.

Elija uno de los siguientes métodos de verificación:

- Registro TXT de DNS: demuestre la propiedad del dominio creando un registro TXT de DNS con su proveedor de DNS.
- Ruta HTTP: demuestre la propiedad del dominio creando una ruta en su servidor web que contenga un token único proporcionado por AWS Security Agent.
- VPC privada: solo se puede utilizar para pruebas de penetración de VPC privadas. Comprueba que el dominio se resuelve en una IP de un rango de CIDR privado. El nombre de dominio configurado debe coincidir con el nombre de dominio completo de todos los puntos finales de destino asociados

Paso 2: Verificar la propiedad del dominio

Tras añadir el dominio, verifica la propiedad mediante el método que hayas seleccionado. Para activar la verificación en cualquier momento desde la tabla Dominios de destino, seleccione el dominio y elija Verificar.

Realice la verificación mediante un registro TXT de DNS

AWS Security Agent genera un valor de registro DNS TXT. Debe añadir este registro a su proveedor de DNS para demostrar su propiedad.

Si el dominio está registrado en Route 53 (la misma cuenta de AWS):

AWS Security Agent puede crear el registro DNS automáticamente. Seleccione el dominio en la tabla de dominios de destino y elija la One-click verificación. AWS Security Agent crea el registro de validación de DNS y completa la verificación automáticamente.

Si el dominio está registrado con otro proveedor de DNS:

1. Copie el valor del registro TXT proporcionado por AWS Security Agent.
2. Añada el registro TXT a su registrador de DNS.
3. Vuelva a la tabla Dominios de destino, seleccione el dominio y elija Verificar.

Verifique mediante la validación de rutas HTTP

Este método demuestra la propiedad del dominio al colocar un token único en su servidor web. Solo los propietarios de dominios o los administradores web autorizados pueden crear rutas en un servidor web, lo que demuestra su propiedad.

1. Cree un archivo en la siguiente ruta de su servidor web:

```
.well-known/aws/securityagent-domain-verification.json
```

2. Coloque el token proporcionado por AWS Security Agent en el archivo con este formato:

```
{
  "tokens": ["<insert-token>"]
}
```

3. Vuelva a la tabla de dominios de destino, seleccione el dominio y elija Verificar. El agente de seguridad de AWS envía una solicitud GET de HTTPS a la URL de verificación y valida el token.

4. Si se puede acceder al dominio en la Internet pública, asegúrese de que su dominio tenga un certificado SSL válido antes de realizar la verificación.

> **Note**
>
> Si tu dominio está registrado en varios espacios de agentes y utilizas la validación de rutas HTTP, puedes colocar los tokens de ambos espacios de agentes en la misma `tokens` matriz.

Omite la verificación de propiedad del dominio

Los clientes que estén autorizados a realizar pruebas de penetración en un terminal pero no puedan completar la verificación de propiedad pueden solicitarnos la verificación manual. Abre un caso de atención al cliente para realizar esta solicitud. Su solicitud debe incluir su caso de uso empresarial y su justificación para la verificación manual de la propiedad (es decir, por qué está autorizado a realizar pruebas de penetración en el terminal).

Dominios objetivo gestionados utilizados para las pruebas de penetración

En la consola de administración de AWS, puede añadir y administrar los dominios de destino que consumen los espacios de los agentes para las pruebas de penetración. Estos dominios de destino deberán verificarse antes de poder utilizarlos en una prueba de penetración. Para obtener más información sobre la verificación de los dominios de destino, consulte the section called “Habilitar la prueba de penetración”

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

1. Prueba de penetración habilitada (consultethe section called “Habilitar la prueba de penetración”)

Gestione los recursos del dominio de destino

- Navegue a la página de información general de los dominios de destino.
- Deberías ver todos los recursos del dominio de destino asociados a tu cuenta
  - Si no ves ningún dominio de destino asociado a tu cuenta, sigue los pasos que se indican the section called “Habilitar la prueba de penetración” para crear y verificar un dominio de destino

- Los dominios de destino se pueden reutilizar entre los espacios de los agentes y comparten el estado de verificación
  - Para añadir un dominio de destino existente a un espacio de agentes, vaya a la pestaña Prueba de penetración del espacio de agentes. Seleccione Agregar dominio y elija el dominio deseado en Seleccione entre los dominios previamente registrados disponibles en el campo de nombre de dominio
  - Los dominios de destino deben estar asociados a un espacio de agente antes de poder utilizarlos en una prueba de penetración
- Al eliminar un dominio de un espacio de agentes, no se elimina el dominio. El dominio de destino asociado se puede eliminar permanentemente de la página de descripción general de los dominios de destino

Compruebe los dominios de destino

Para que un dominio de destino se utilice en una prueba de penetración, primero debe verificarse mediante uno de los siguientes métodos:

- Dominios de Route 53 (la misma cuenta de AWS): elige la One-click verificación. AWS Security Agent crea automáticamente el registro DNS y completa la verificación.
- DNS TXT (otros proveedores de DNS): copie el token de verificación, añada el registro TXT a su registrador de DNS, seleccione el dominio y elija Verificar.
- Ruta HTTP: coloca el token de verificación en la ruta requerida de tu servidor web, selecciona el dominio y elige Verificar. Para obtener más información, consulte the section called “Habilitar un dominio de aplicación para las pruebas de penetración”.
- VPC privada: verifica que la IP del dominio de destino se encuentre dentro de un rango de CIDR privado (consulte the section called “Conectar el agente a los recursos de VPC privados” para obtener una lista de los rangos de CIDR privados). El nombre del dominio del punto final de la prueba de penetración debe coincidir con el nombre de dominio completo configurado para la verificación. Solo se puede utilizar para pruebas de penetración de VPC privadas

> **Note**
>
> Para la verificación de DNS TXT, ruta HTTP y Route 53, los subdominios de un dominio verificado se cubren automáticamente y no requieren una verificación por separado. Para la verificación de la VPC privada, cada dominio debe verificarse de forma individual.

Gestione los requisitos de seguridad

Defina los requisitos de seguridad que AWS Security Agent evalúa durante las revisiones del diseño y el código mediante AWS-managed paquetes, paquetes personalizados o requisitos importados de su propia documentación.

Gestione los requisitos de seguridad

Organice los requisitos de AWS seguridad que Security Agent utiliza para analizar sus aplicaciones en paquetes de requisitos de seguridad. Un paquete es un conjunto de requisitos de seguridad. Puede activar los paquetes AWS gestionados, crear sus propios paquetes personalizados y generar los requisitos para un paquete personalizado cargando su documentación de seguridad.

Descripción general de

Un requisito de seguridad define una norma o política de seguridad con la que AWS Security Agent evalúa su aplicación durante las revisiones del diseño y del código. Cuando un diseño o un código no cumple con un requisito, AWS Security Agent informa de su hallazgo. Cada requisito de seguridad pertenece a un paquete de requisitos de seguridad. Los requisitos de seguridad se comparten en todos los espacios de agentes y se evalúan durante las revisiones del diseño y el código.

AWS Security Agent ofrece dos tipos de paquetes, que se muestran en pestañas separadas:

- Paquetes de requisitos de seguridad AWS gestionados: paquetes de requisitos de seguridad proporcionados según los estándares y las mejores prácticas del sector. Puede habilitar estos paquetes al instante para que los evalúen en función de las políticas de seguridad habituales sin necesidad de una configuración personalizada. Los requisitos de un paquete gestionado son de solo lectura. Puede utilizar un requisito AWS gestionado como plantilla para un requisito personalizado. Para ver la lista de paquetes gestionados disponibles, consulte los paquetes de requisitos de seguridad AWS gestionados.
- Paquetes de requisitos de seguridad personalizados: paquetes que se crean para hacer cumplir las políticas y estándares específicos de su organización. Los requisitos se crean desde cero en un paquete personalizado, se personalizan los requisitos AWS gestionados como punto de partida o se generan cargando la documentación de seguridad.

> **Note**
>
> Los paquetes de marcos de conformidad están diseñados para ayudar a identificar los requisitos de seguridad que pueden ser relevantes para el cumplimiento de determinados marcos. No evalúan su cumplimiento ni garantizan que supere una auditoría.

Los paquetes se activan y desactivan como una unidad. Cuando un paquete está activado, AWS Security Agent evalúa sus aplicaciones en función de los requisitos de ese paquete durante las revisiones de diseño y código.

> **Note**
>
> La activación o desactivación de un paquete se aplica a las nuevas revisiones de diseño y de código. Las revisiones existentes no se ven afectadas.

Habilita o deshabilita un paquete gestionado

Habilite un paquete AWS administrado para evaluar sus aplicaciones en función de un conjunto de requisitos AWS de seguridad mantenidos. Desactívelo cuando ya no lo necesite.

1. En la AWS consola, vaya a AWS Security Agent.
2. En el panel de navegación, selecciona Requisitos de seguridad.
3. Seleccione la pestaña Paquetes de requisitos de seguridad gestionados.
4. Seleccione el paquete que desee activar o desactivar.
5. Realice una de las siguientes acciones:
   a. Para activar el paquete, selecciona Activar paquete.
   b. Para deshabilitar el paquete, selecciona Desactivar paquete.

> **Tip**
>
> Elija un paquete para ver los requisitos de seguridad que contiene. Elija un requisito para ver su definición completa, incluida su aplicabilidad, los criterios de conformidad y la guía de corrección.

Cree un paquete personalizado

Cree un paquete personalizado para agrupar los requisitos de seguridad específicos de su organización. Después de crear el paquete, añada requisitos manualmente, personalice un requisito AWS gestionado o cargue documentos para generar requisitos.

1. En la AWS consola, vaya a AWS Security Agent.
2. En el panel de navegación, selecciona Requisitos de seguridad.
3. Seleccione la pestaña Paquetes de requisitos de seguridad personalizados.
4. Seleccione Crear paquete de requisitos de seguridad.
5. Introduzca el nombre del paquete de requisitos de seguridad y una descripción opcional.
6. Seleccione Crear paquete de requisitos de seguridad.

> **Note**
>
> Tras crear un paquete, puede añadir o cargar los documentos fuente para generar los requisitos de seguridad del paquete.

Añada un requisito de seguridad manualmente

Agregue un requisito de seguridad a un paquete personalizado para definir un estándar de seguridad que AWS Security Agent aplique.

1. En la AWS consola, vaya a AWS Security Agent.
2. En el panel de navegación, selecciona Requisitos de seguridad.
3. Seleccione la pestaña Paquetes de requisitos de seguridad personalizados y, a continuación, elija el paquete al que desee añadir un requisito.
4. Seleccione Añadir requisito manualmente.
5. Configure los siguientes campos:
   a. Nombre del requisito de seguridad: introduzca un nombre descriptivo que identifique el control de seguridad, por ejemplo `enforce-encryption-at-rest` (80 caracteres como máximo).
   b. Descripción: proporcione una breve descripción de lo que comprueba este requisito de seguridad (500 caracteres como máximo).

c. Aplicabilidad: describa los escenarios, los tipos de sistema o las condiciones en los que se debe evaluar este requisito de seguridad. Incluya los escenarios en los que el requisito debe marcarse como NOT_APPLICABLE (máximo 10 000 caracteres).

d. Criterios de conformidad: defina qué constituye conformidad o incumplimiento en relación con este requisito de seguridad. Proporcione los indicadores, ejemplos y detalles técnicos que AWS Security Agent busca al evaluar el cumplimiento (máximo 10 000 caracteres).

e. Guía de corrección (opcional): proporcione orientación sobre cómo corregir las infracciones, incluidos enlaces a la documentación o los estándares internos de su organización (máximo 10 000 caracteres).

6. Realice una de las siguientes acciones:

a. Para crear el requisito sin habilitarlo, elija Crear requisito de seguridad.

b. Para crear el requisito y habilitarlo, elija Crear y habilitar el requisito de seguridad.

> **Note**
>
> Un requisito se evalúa durante las revisiones de seguridad solo cuando el paquete que lo contiene está activado. Para controlar si un paquete se evalúa, active o desactive el paquete.

Personalice un AWS-requisito de seguridad gestionado

Cree un requisito de seguridad personalizado que utilice un requisito AWS gestionado como punto de partida. AWS Security Agent rellena previamente los detalles del requisito gestionado y usted los edita para adaptarlos a su organización.

1. En la AWS consola, vaya a AWS Security Agent.
2. En el panel de navegación, selecciona Requisitos de seguridad.
3. Seleccione la pestaña Paquetes de requisitos de seguridad personalizados y, a continuación, elija el paquete personalizado al que desee añadir el requisito.
4. Seleccione Crear un requisito de seguridad personalizado.
5. Para rellenar previamente el formulario, en la sección Personalizar un requisito AWS de seguridad gestionado, busque y seleccione un requisito AWS gestionado para utilizarlo como plantilla.
6. Edite cualquiera de los campos para adaptarlos a las necesidades de su organización.
7. Realice una de las siguientes acciones:

a. Para crear el requisito sin habilitarlo, elija Crear requisito de seguridad.
b. Para crear y habilitar inmediatamente el requisito, elija Crear y habilitar el requisito de seguridad.

> **Note**
>
> La personalización de un requisito AWS gestionado crea un requisito de seguridad personalizado e independiente. Los cambios posteriores en el requisito AWS-administrado no afectan a la versión personalizada.

Genere requisitos cargando documentos

Genere los requisitos de seguridad para un paquete personalizado a partir de la documentación de seguridad existente en lugar de escribir cada requisito a mano. AWS Security Agent lee los documentos que subes, identifica el contenido relevante para la seguridad y genera requisitos estructurados que puedes revisar y editar. Para ver el procedimiento completo, consulte Generar requisitos de seguridad a partir de documentos. Para obtener información sobre qué incluir en los documentos que suba, consulte Preparar los documentos para la generación de requisitos.

> **Important**
>
> Al cargar nuevos documentos fuente se regeneran todos los requisitos del paquete. Se sustituyen todos los requisitos existentes, incluidos los que haya agregado manualmente.

Edite un requisito de seguridad personalizado

Modifique un requisito de seguridad personalizado para actualizar su definición, criterio o guía de corrección. No puede editar los requisitos de un paquete AWS gestionado.

1. En la AWS consola, vaya a AWS Security Agent.
2. En el panel de navegación, selecciona Requisitos de seguridad.
3. Seleccione la pestaña Paquetes de requisitos de seguridad personalizados y, a continuación, elija el paquete que contiene el requisito.
4. Seleccione el requisito que desee editar y, a continuación, elija Editar requisito de seguridad personalizado.

5. Actualice los campos de requisitos según sea necesario. El nombre del requisito de seguridad no se puede cambiar después de su creación.
6. Seleccione Actualizar el requisito de seguridad.

> **Note**
>
> Los cambios en un requisito de seguridad se aplican a las revisiones de nuevos diseños y códigos. Las revisiones existentes no se ven afectadas.

Habilita o deshabilita un paquete

Habilite o deshabilite un paquete de requisitos de seguridad para controlar si AWS Security Agent evalúa los requisitos que contiene. Los paquetes se activan y desactivan como una unidad.

1. En la AWS consola, vaya a AWS Security Agent.
2. En el panel de navegación, selecciona Requisitos de seguridad.
3. Elija la pestaña correspondiente al tipo de paquete y, a continuación, seleccione el paquete.
4. Realice una de las siguientes acciones:
   a. Para activar el paquete, selecciona Activar paquete.
   b. Para deshabilitar el paquete, selecciona Desactivar paquete.

> **Note**
>
> Cuando un paquete está activado, los requisitos del paquete se evalúan durante las revisiones de seguridad. Cuando un paquete está desactivado, no se evalúan sus requisitos.

Elimine un requisito de seguridad personalizado

Elimine un requisito de seguridad personalizado cuando ya no desee que AWS Security Agent lo evalúe.

1. En la AWS consola, vaya a AWS Security Agent.
2. En el panel de navegación, selecciona Requisitos de seguridad.

3. Seleccione la pestaña Paquetes de requisitos de seguridad personalizados y, a continuación, elija el paquete que contiene el requisito.
4. Seleccione uno o más requisitos de seguridad y, a continuación, elija Eliminar requisito de seguridad.
5. Confirme la eliminación.

> **Note**
>
> Al eliminar los requisitos de seguridad, dejarán de evaluarse en futuras revisiones. Los requisitos permanecen visibles en las revisiones anteriores como resultados de solo lectura.

Mejores prácticas para definir los requisitos de seguridad

Al crear un requisito de seguridad, siga estas pautas para ayudar a AWS Security Agent a evaluar sus aplicaciones con precisión y proporcionar resultados procesables.

Nombre del requisito de seguridad: utilice un nombre claro y específico que identifique el control de seguridad. Evite los términos genéricos que no expresen el propósito del requisito.

Descripción: explique lo que comprueba el control y el riesgo que mitiga. Esto ayuda a los usuarios a entender por qué es importante el requisito.

Aplicabilidad: describa las cargas de trabajo, los tipos de sistemas o las condiciones en las que se debe evaluar el requisito. Indique cuándo debe marcarse el requisito como NOT_APPLICABLE, con escenarios específicos, para evitar falsos positivos. Frases como «Este control se aplica a TODAS las cargas de trabajo que...» y «Marcar como NO APLICABLE si...» establecen límites de alcance claros.

Criterios de cumplimiento: estructura esto en dos partes: qué demuestra el cumplimiento y qué indica el incumplimiento. Sea específico con los indicadores técnicos e incluya casos extremos. Comience con «Un diseño es conforme si demuestra que...» seguido de los detalles técnicos y, a continuación, «Un diseño no es conforme si...», con los patrones que indican una infracción.

Guía de corrección: proporcione orientación con detalles técnicos y ejemplos de configuración. Incluya enlaces a la documentación interna de su organización para que los desarrolladores dispongan de los recursos que necesitan para corregir las infracciones.

Siguientes pasos

Después de configurar los paquetes de requisitos de seguridad:

- Cree una revisión del diseño o del código para evaluar su aplicación con respecto a los paquetes que ha activado.
- Habilite las pruebas de penetración para complementar sus revisiones de diseño y código.
- Conceda a los usuarios acceso a la aplicación web AWS Security Agent.

Paquetes de requisitos de seguridad gestionados por AWS

Un paquete de requisitos de seguridad AWS gestionados es un conjunto de requisitos de seguridad que se AWS crean y mantienen en función de los estándares y las mejores prácticas del sector. Usted habilita un paquete gestionado para evaluar sus aplicaciones en función de sus requisitos durante las revisiones del diseño y del código, sin tener que escribir los requisitos usted mismo.

Los requisitos de seguridad de un paquete gestionado son de solo lectura. No puede cambiarlos. Puede utilizar un requisito AWS gestionado como plantilla para crear un requisito personalizado y, a continuación, editar la copia para adaptarla a su organización. Para obtener más información, consulte Administrar los requisitos de seguridad.

AWS actualiza los paquetes gestionados a lo largo del tiempo. Al AWS añadir o revisar un requisito en un paquete gestionado, el cambio se aplica a todas las cuentas que tengan el paquete activado.

> **Note**
>
> Los paquetes de marcos de cumplimiento están diseñados para ayudar a identificar los requisitos de seguridad que pueden ser relevantes para el cumplimiento de ciertos marcos. No evalúan su cumplimiento ni garantizan que supere una auditoría.

Paquete gestionado por AWS: paquete base ASA

Un conjunto básico de requisitos de seguridad que se aplican a la mayoría de las cargas de trabajo. Este paquete cubre los problemas de seguridad más comunes de las aplicaciones, como la autenticación y la autorización, la protección de datos, el registro y la validación de las entradas. Activa este paquete para establecer una base de seguridad para tus revisiones de diseño y código.

Paquete gestionado por AWS: Well-Architected paquete AWS

Requisitos de seguridad derivados del pilar de seguridad del AWS Well-Architected Framework. Este paquete evalúa su aplicación según las AWS directrices para proteger los datos, administrar las identidades y los permisos y detectar los eventos de seguridad y responder a ellos. Para obtener más información sobre el marco, consulte Security Pillar: AWS Well-Architected Framework.

Paquete gestionado por AWS: paquete NIST CSF

Requisitos de seguridad derivados del marco de ciberseguridad (CSF) del NIST. Este paquete evalúa su aplicación en función de las áreas de control derivadas del marco, como la gestión de identidades y accesos, la seguridad de los datos y la tecnología de protección. Utilice este paquete para alinear sus revisiones de diseño y código con el CSF del NIST.

Paquete gestionado por AWS: paquete PCI DSS

Requisitos de seguridad derivados del estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS). Este paquete evalúa su solicitud comparándola con las áreas de control relevantes para el manejo de los datos de los titulares de tarjetas, como el control de acceso, el cifrado de los datos en tránsito y en reposo y el registro. Utilice este paquete para alinear sus revisiones de diseño y código con el PCI DSS.

Genere requisitos de seguridad a partir de documentos

Genera los requisitos de seguridad para un paquete personalizado cargando la documentación de seguridad existente. AWS Security Agent lee los documentos que subes, identifica el contenido relevante para la seguridad y genera requisitos de seguridad estructurados con su aplicabilidad, criterios de conformidad y directrices de corrección. Puede revisar y editar los requisitos generados antes de utilizarlos en las revisiones.

Utilice esta opción en lugar de escribir cada requisito a mano si ya tiene documentadas las políticas, normas o directrices de seguridad. Para obtener orientación sobre qué incluir en los documentos que suba, consulte Preparar documentos para la generación de requisitos.

Formatos de archivo compatibles

Puede cargar los siguientes formatos de archivo:

- DOC
- DOCX

- MD
- PDF
- TXT

Genera requisitos

1. En la AWS consola, vaya a AWS Security Agent.
2. En el panel de navegación, selecciona Requisitos de seguridad.
3. Seleccione la pestaña Paquetes de requisitos de seguridad personalizados.
4. Cree un paquete o elija uno personalizado existente para generar los requisitos.
5. Selecciona Elegir archivos o arrastra y suelta tus documentos en el área de carga.
6. Selecciona Generar requisitos.
7. Espere a que AWS Security Agent procese los documentos. La generación se ejecuta en segundo plano y puede tardar un par de minutos en el caso de archivos grandes. No puedes iniciar otra carga para el paquete mientras la generación esté en curso.
8. Revisa los requisitos de seguridad generados. Edite, elimine o añada los requisitos según sea necesario. Active el paquete cuando desee que AWS Security Agent evalúe sus requisitos durante las revisiones de seguridad.

> **Note**
>
> AWS Security Agent genera requisitos a nivel de carga de trabajo y se centra en el contenido relevante para la seguridad de sus documentos. La cantidad de requisitos que genera depende del contenido que proporcione. Revisa los requisitos generados para confirmar que reflejan tu intención.

Sustituya los requisitos por una nueva subida

Al cargar nuevos documentos fuente, se regeneran los requisitos de un paquete.

> **Important**
>
> Al cargar nuevos documentos fuente a un paquete, AWS Security Agent regenera todos los requisitos de ese paquete. Se sustituyen todos los requisitos existentes, incluidos los que

haya agregado manualmente. Para mantener sus requisitos actuales, no cargue documentos nuevos.

1. En la AWS consola, vaya a AWS Security Agent.
2. En el panel de navegación, selecciona Requisitos de seguridad.
3. Seleccione la pestaña Paquetes de requisitos de seguridad personalizados y, a continuación, elija el paquete.
4. Inicie una nueva carga y reconozca que la carga de nuevos documentos fuente reemplaza los requisitos existentes.
5. Elija sus archivos y, a continuación, elija Generar requisitos.

Siguientes pasos

- Revise y active los requisitos generados. Consulte Administrar los requisitos de seguridad.
- Cree una revisión del diseño o del código para evaluar su aplicación en comparación con el resto.

Prepare los documentos para la generación de requisitos

Al generar requisitos de seguridad a partir de documentos, AWS Security Agent lee los documentos y genera requisitos estructurados a partir del contenido relevante para la seguridad que encuentra. No es necesario formatear los documentos de ninguna manera en particular ni escribir previamente la aplicabilidad, los criterios de conformidad y las directrices de corrección. AWS Security Agent las obtiene del contenido que usted proporciona. Cargue la documentación de seguridad que ya tiene, escrita con sus propias palabras.

En esta página se describe lo que se debe incluir para que AWS Security Agent genere requisitos precisos y útiles. Para conocer el procedimiento de carga y los límites de los archivos, consulte Generar requisitos de seguridad a partir de documentos.

¿Qué incluir

AWS Security Agent busca contenido que describa sus expectativas de seguridad. Los documentos que tratan los siguientes temas generan los requisitos más estrictos:

- Control de acceso y autorización

- Autenticación
- Protección y cifrado de datos
- Seguridad de la red
- Registro y auditoría
- Respuesta a incidentes
- Administración de vulnerabilidades y parches
- Obligaciones de cumplimiento que se aplican a sus cargas de trabajo

Entre los buenos documentos fuente se incluyen las políticas de seguridad, las normas de ingeniería, los catálogos de control, las directrices de arquitectura y los estándares de codificación segura.

Escribe al nivel de la carga de trabajo

AWS Security Agent genera requisitos que se aplican a una carga de trabajo o aplicación individual, el mismo ámbito que evalúa durante las revisiones del diseño y el código. El contenido que describe cómo crear y operar una carga de trabajo segura genera requisitos. Organization-wide Los temas de gobierno, como la estrategia de múltiples cuentas, la administración de usuarios raíz y la configuración del registro a nivel de cuenta, quedan fuera de este ámbito y no generan requisitos de carga de trabajo.

Describa el resultado, no una sola implementación

Indique el resultado de seguridad que espera en lugar de un solo producto o configuración prescritos. AWS Security Agent genera requisitos que se centran en la capacidad de seguridad necesaria y permiten más de una implementación válida. Por ejemplo, «los datos en reposo están cifrados» genera un requisito más claro y de aplicación más amplia que una declaración que menciona un servicio o entorno específico.

Sea específico acerca de cómo se ve lo bueno

Cuanto más concretamente describan sus documentos el comportamiento esperado, mejor podrá definir AWS Security Agent los criterios de conformidad. Siempre que pueda, describa lo que demuestra un diseño compatible y lo que indica una infracción. Las declaraciones vagas o meramente ambiciosas generan menos requisitos y son más débiles que los requisitos concretos y relevantes para la carga de trabajo.

Revisa lo que recibas a cambio

Cada requisito generado incluye un nombre, una aplicabilidad, unos criterios de conformidad y una guía de corrección que AWS Security Agent ha extraído de sus documentos. Revise los requisitos generados, edite los que necesiten ajustes y active los que desee que AWS Security Agent evalúe. Para obtener más información, consulte Administrar los requisitos de seguridad.

Gestione los usuarios y el acceso

Controle quién puede acceder a cada espacio de agente y configure las funciones de IAM y las claves de cifrado que utiliza AWS Security Agent.

Otorgue a los usuarios acceso a la aplicación web AWS Security Agent

AWS Security Agent proporciona dos métodos para que los usuarios accedan a la aplicación web, en función de cómo haya configurado su espacio de agente durante la configuración.

Descripción general de los métodos de acceso

Centro de identidad de IAM (SSO): si ha activado el Centro de identidad de IAM al crear su espacio de agente, los usuarios pueden acceder a la aplicación web directamente a través del SSO. Los usuarios se asignan al espacio de agentes a través de la consola de AWS Security Agent y los usuarios inician sesión con sus credenciales de Identity Center.

Acceso de administrador: los usuarios con acceso a la consola de AWS pueden lanzar la aplicación web a través de un enlace de acceso de administrador en la página de información general del espacio de agentes de la consola de administración de AWS.

Conceda acceso con el Centro de Identidad de IAM (SSO)

Si configuró su espacio de agente con el Centro de identidad de IAM, puede asignar usuarios al espacio de agente mediante la consola de AWS Security Agent.

Asigne usuarios a través de la consola de AWS Security Agent

1. En la consola de administración de AWS Security Agent, vaya a su espacio de agente.
2. Seleccione la pestaña de la aplicación web.
3. En la tabla Usuarios, elija Agregar usuarios.

4. Seleccione los usuarios existentes en el Centro de identidades de IAM o cree nuevos usuarios.
5. Confirme las asignaciones de usuarios.

> **Tip**
>
> Los usuarios asignados al Agent Space pueden acceder a la aplicación web iniciando sesión a través del IAM Identity Center con sus credenciales de inicio de sesión único.

Acceda a la aplicación web con el inicio de sesión único

Una vez asignados los usuarios al espacio de agentes:

1. Los usuarios navegan hasta la URL de la aplicación web del espacio de agentes.

   > **Tip**
   >
   > Busque la URL de la aplicación web en la página de detalles de Agent Space en la consola de AWS Security Agent seleccionando Copiar la URL de la aplicación web. Los usuarios deben marcar esta URL como favorita para acceder a ella fácilmente.

2. Los usuarios inician sesión con sus credenciales de inicio de sesión único.
3. Tras la autenticación, los usuarios pueden seleccionar el espacio de agentes y empezar a realizar evaluaciones de seguridad.

Conceda acceso con IAM-only acceso

Si configuró su espacio de agente con IAM-only acceso, los usuarios con acceso a la consola AWS pueden lanzar la aplicación web a través de un enlace de acceso de administrador.

Utilice el enlace de acceso de administrador

1. Inicie sesión en la consola de AWS Security Agent.
2. Navegue hasta el espacio de agentes al que desee acceder.
3. En la pestaña de aplicaciones web de la página de inicio de Agent Space, pulse el botón de acceso de administrador para iniciar la aplicación web.
4. La aplicación web se abre en una nueva pestaña y el usuario se autentica automáticamente.

> **Note**
>
> El enlace de acceso de administrador solo está disponible para los usuarios que ya se hayan autenticado en la consola de AWS con los permisos de AWS Security Agent correspondientes. Este método no requiere la configuración del centro de identidad de IAM.

Siguientes pasos

Tras conceder a los usuarios el acceso a la aplicación web:

- Los usuarios pueden crear y gestionar las configuraciones y ejecuciones de las pruebas de penetración
- Los usuarios pueden crear y gestionar revisiones de diseño
- Los usuarios pueden ver los hallazgos de seguridad y la guía de corrección
- Configure las preferencias de notificación para los hallazgos de seguridad

Crear un rol de IAM para el agente de seguridad de AWS

El agente de seguridad de AWS utiliza las funciones de IAM de tres maneras:

1. Función de aplicación: se utiliza al crear la aplicación AWS Security Agent. En los casos de uso del centro de identidad de IAM y del enlace de acceso de administrador, el servicio asume esta función para conceder a WebApp los usuarios permisos para interactuar con las API de AWS Security Agent.
2. Función del servicio de pruebas de penetración: se especifica al crear espacios de agentes como una lista de funciones disponibles. Más adelante, WebApp los usuarios seleccionan uno de estos roles al crear una prueba de penetración. El servicio AWS Security Agent asume esta función para acceder a los recursos de AWS durante las pruebas.
3. Función de actor: se utiliza para autenticar y autorizar las solicitudes a la aplicación web de destino (por ejemplo, las API API Gateway de AWS). Estas funciones se proporcionan durante la creación del espacio de agentes. El agente de seguridad de AWS asume funciones de actor para interactuar con la aplicación de destino.

Rol de aplicación

El rol de aplicación se utiliza al crear la aplicación AWS Security Agent en el servicio. En los escenarios de autenticación del centro de identidad de IAM y del enlace de acceso de administrador, el servicio AWS Security Agent asume esta función para conceder a WebApp los usuarios los permisos necesarios para interactuar con las API de AWS Security Agent.

Permisos necesarios

Este rol necesita permisos para:

- Invoque las operaciones de la API de AWS Security Agent
- Lea y escriba los datos de configuración de la aplicación
- Acceda a la información de la sesión del usuario
- Administre los tokens de autenticación para WebApp los usuarios

Política de confianza

La política de confianza debe permitir que el servicio AWS Security Agent asuma esta función:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Política de permisos

El rol debe incluir permisos para:

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "securityagent:GetApplication",
        "securityagent:UpdateApplication",
        "securityagent:ListAgentInstances",
        "securityagent:CreatePentestSession"
      ],
      "Resource": "arn:aws:securityagent:*:*:application/*"
    }
  ]
}
```

> **Note**
>
> Personalice los permisos en función de los requisitos específicos de su aplicación y del principio de privilegio mínimo.

Función del servicio de pruebas de penetración

El rol del servicio de pruebas de penetración se especifica al crear espacios de agentes como una lista de roles disponibles. Cuando WebApp los usuarios crean una prueba de penetración, seleccionan uno de estos roles. A continuación, el servicio AWS Security Agent asume esta función para acceder a los recursos de AWS y probarlos.

Permisos necesarios

Este rol necesita permisos para acceder a sus recursos de AWS y analizarlos durante las pruebas de penetración:

- Lea y describa las configuraciones de VPC y la topología de red
- Inspeccione las instancias, los grupos de seguridad y las ACL de red de EC2
- Analice las políticas de IAM y los permisos de recursos
- Lea CloudWatch los registros y las métricas
- Acceda a las configuraciones de servicios de AWS relevantes para las pruebas de seguridad

Política de confianza

La política de confianza debe permitir que el servicio AWS Security Agent asuma esta función en las operaciones de pruebas de penetración:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "your-external-id"
        }
      }
    }
  ]
}
```

> **Note**
>
> Utilice un ID externo como medida de seguridad adicional cuando permita el acceso entre cuentas o servicios.

Política de permisos

El rol debe incluir acceso de solo lectura a sus recursos de AWS. Considere la posibilidad de utilizar estas políticas administradas:

- `SecurityAudit`- Política gestionada por AWS para la auditoría de seguridad
- `ViewOnlyAccess`- Read-only acceso a la mayoría de los servicios de AWS

O cree una política personalizada con permisos específicos:

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:Describe*",
        "vpc:Describe*",
        "iam:Get*",
        "iam:List*",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "*"
    }
  ]
}
```

Important

Concede solo los permisos mínimos necesarios para el alcance de tus pruebas de penetración. Revise y ajuste los permisos en función de los servicios de AWS que desee incluir en las pruebas de seguridad.

Rol de actor

El rol de actor se utiliza para autenticar y autorizar las solicitudes a la aplicación web de destino durante las pruebas de penetración. Estas funciones se proporcionan durante la creación del espacio de agentes y el agente de AWS Security Agent las asume para interactuar con los puntos de enlace de la aplicación de destino (como las API de API Gateway de AWS, las URL de funciones de Lambda u AWS-hosted otras aplicaciones).

Permisos necesarios

Este rol necesita permisos para:

- Invocar puntos finales de API Gateway

- Ejecute funciones Lambda
- Acceda a los recursos de AWS específicos de cada aplicación
- Autentíquese con los mecanismos de autenticación de la aplicación de destino
- Realice operaciones HTTP en los puntos finales de su aplicación

Política de confianza

La política de confianza debe permitir que el servicio de agentes de AWS Security Agent asuma esta función:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "your-external-id"
        }
      }
    }
  ]
}
```

Política de permisos

Los permisos dependen de la arquitectura de la aplicación de destino. A continuación, se muestran ejemplos de escenarios comunes:

Para aplicaciones API Gateway

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

```
      "Action": [
        "execute-api:Invoke"
      ],
      "Resource": "arn:aws:execute-api:us-east-1:*:your-api-id/*"
    }
  ]
}
```

Para las direcciones URL de funciones Lambda

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lambda:InvokeFunctionUrl",
        "lambda:InvokeFunction"
      ],
      "Resource": "arn:aws:lambda:us-east-1:*:function:your-function-name"
    }
  ]
}
```

Para Application Load Balancer con Autenticación de Cognito

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cognito-idp:InitiateAuth",
        "cognito-idp:RespondToAuthChallenge"
      ],
      "Resource": "arn:aws:cognito-idp:us-east-1:*:userpool/your-user-pool-id"
    }
  ]
}
```

> **Important**
>
> Configure los permisos de Actor Role para que coincidan con los requisitos de autenticación y autorización de la aplicación de destino. El rol debe tener el mismo nivel de acceso que los usuarios o servicios que el agente de seguridad simulará durante las pruebas de penetración.

Claves administradas por el cliente para AWS Security Agent

De forma predeterminada, AWS Security Agent cifra todos los datos en reposo mediante claves de cifrado AWS administradas. Si lo desea, puede utilizar una clave gestionada por el cliente del Servicio de administración de AWS claves (AWS KMS) para cifrar sus datos, lo que le proporciona un control total sobre las claves de cifrado que protegen sus recursos.

AWS Security Agent admite claves administradas por el cliente a nivel de recursos. Al crear un recurso de nivel superior, como un espacio de agente o una integración, puede especificar una clave KMS para cifrar todos los datos que pertenecen a ese recurso y sus subrecursos. Por ejemplo, si se especifica una clave gestionada por el cliente al crear un Agent Space, se cifran todos los datos asociados a ese Agent Space, incluidas las configuraciones de Agent Space, las configuraciones de las pruebas de penetración, los trabajos y los detalles de ejecución, los datos de seguridad, los puntos finales descubiertos y las capturas de pantalla. También puedes proporcionar AWS recursos que ya estén cifrados con tu propia clave gestionada por el cliente, como depósitos de S3, grupos de CloudWatch registros de Logs o secretos de Secrets Manager. Para conocer los permisos de KMS necesarios, consultethe section called “Permisos de KMS necesarios”.

Cómo funcionan las claves administradas por el cliente

AWS Security Agent utiliza el conjunto de claves jerárquicas del AWS KMS para cifrar los datos con claves administradas por el cliente. Cuando especificas una clave de KMS durante la creación del recurso, el servicio crea una clave de sucursal protegida por tu clave de KMS y la almacena en un almacén de DynamoDB-based claves de Amazon. Para cada operación de cifrado, el conjunto de claves jerárquico obtiene una clave de empaquetado única de la clave de sucursal activa, que cifra una clave de cifrado de datos única para cada solicitud.

El anillo de claves jerárquico ofrece las siguientes ventajas:

- Per-resource ámbito de cifrado: cada recurso de nivel superior tiene su propia clave de rama, por lo que los datos de los distintos recursos se cifran con claves independientes.

- Rotación automática de claves: AWS Security Agent rota periódicamente las claves de ramificación. Tras la rotación, los datos nuevos se cifran con la nueva versión de la clave de rama, mientras que las versiones anteriores se conservan para descifrar los datos previamente cifrados.

Contexto de cifrado

AWS Security Agent utiliza el contexto de cifrado en todas las operaciones criptográficas con su clave KMS. El contexto de cifrado es un conjunto de pares clave-valor no secretos que proporciona datos autenticados adicionales para la operación de cifrado.

La clave de contexto de cifrado sigue el formato`aws:securityagent:_<resource-type>_`, *`<resource-type>`* es decir, el tipo de recurso que se va a cifrar (por ejemplo, o). `agent-space` `integration` El valor es el nombre de recurso de Amazon (ARN) del recurso.

> **Note**
>
> En el caso de las integraciones, la clave de contexto de cifrado incluye el `aws-crypto-ec:` prefijo, lo que da como resultado el formato. `aws-crypto-ec:aws:securityagent:integration`

Puede usar el contexto de cifrado para limitar su política de claves de KMS a tipos de recursos específicos. Para obtener más información, consulte the section called “Permisos de KMS necesarios”.

Default encryption (Cifrado predeterminado)

Cuando crea un recurso sin especificar una clave administrada por el cliente, AWS Security Agent cifra el recurso mediante claves de cifrado AWS administradas que proporcionan los servicios de almacenamiento subyacentes (Amazon DynamoDB y Amazon S3). No se requiere ninguna configuración adicional para el cifrado predeterminado.

Clave KMS predeterminada para las aplicaciones

Puede establecer una clave KMS predeterminada a nivel de aplicación. Cuando se configura una clave KMS predeterminada, AWS Security Agent la usa como alternativa para nuevos espacios de agente e integraciones cuando no se especifica explícitamente una clave KMS durante la creación del recurso.

Para establecer una clave KMS predeterminada, especifique el `defaultKmsKeyId` parámetro al crear o actualizar la aplicación mediante la AWS CLI o el SDK. La consola le pide que especifique una clave KMS predeterminada durante la configuración de la aplicación.

Cuando se especifica de forma explícita una clave KMS durante la creación del recurso, esta tiene prioridad sobre la predeterminada a nivel de aplicación.

Requisitos previos

Antes de configurar una clave administrada por el cliente, cumpla los siguientes requisitos previos:

- Cree una clave KMS de cifrado simétrico en AWS KMS. La clave debe cumplir los siguientes requisitos:
  - Tipo de clave: simétrica
  - Uso de la clave: cifrar y descifrar
  - Especificación clave: `SYMMETRIC_DEFAULT`
  - Estado clave: activado

  Para obtener instrucciones, consulte Creación de claves en la Guía AWS para desarrolladores del Servicio de administración de claves.
- Configure la política de claves de KMS y las políticas de IAM para conceder a AWS Security Agent los permisos necesarios. Para obtener más información, consulte the section called “Permisos de KMS necesarios”.

Permisos de KMS necesarios

AWS Security Agent requiere permisos de KMS en dos escenarios:

- Cifrado de datos en AWS Security Agent: cuando se especifica una clave gestionada por el cliente para un espacio de agente o una integración, el servicio necesita permisos para utilizar esa clave en las operaciones criptográficas con los datos.
- Uso de CMK-encrypted AWS recursos: cuando proporciona AWS recursos cifrados con una clave administrada por el cliente (como depósitos de S3, grupos de CloudWatch registros de Logs o secretos de Secrets Manager), el servicio necesita permisos para usar esas claves y acceder a los recursos cifrados.

AWS Security Agent accede a la clave KMS con distintas identidades en función de la operación:

- AWS Operaciones de la consola de administración: cuando los administradores crean o administran recursos en la consola de AWS administración (por ejemplo, al crear un espacio de agentes o actualizar una aplicación), el servicio utiliza la función de administrador para llamar a AWS KMS.
- Operaciones de aplicaciones web: cuando los usuarios del IAM Identity Center acceden a los datos a través de la aplicación web AWS Security Agent (por ejemplo, consultan los resultados de las pruebas de penetración o inician una prueba de penetración), el servicio utiliza el rol de aplicación creado durante la configuración del AWS Security Agent para llamar a AWS KMS.
- Acceso a los recursos proporcionados por el cliente: cuando el servicio accede a AWS los recursos proporcionados por el cliente durante las pruebas de penetración (como depósitos de S3, grupos de CloudWatch registros y secretos de Secrets Manager), utiliza la función de servicio de pruebas de penetración para llamar a KMS. AWS
- Flujos de trabajo asíncronos: para las operaciones en segundo plano que se ejecutan fuera de cualquier sesión de usuario (por ejemplo, la ejecución de pruebas de penetración, el procesamiento de revisión de código y la rotación de claves de rama), el servicio utiliza su propio director de servicio (`securityagent.amazonaws.com`) para llamar a AWS KMS en su nombre.

En las siguientes secciones se describen los permisos necesarios para cada identidad.

Política de claves

Su política de claves de KMS debe conceder a AWS Security Agent permiso para usar la clave en operaciones criptográficas. Las declaraciones de política clave requeridas dependen de los tipos de recursos que planee cifrar y de CMK-encrypted AWS los recursos que proporcione al servicio.

Política clave para Agent Spaces

La siguiente política clave otorga a AWS Security Agent los permisos necesarios para cifrar y descifrar los datos de Agent Space, incluidos los resultados de las pruebas de penetración y las capturas de pantalla.

Sustituya los siguientes valores de marcador de posición en la política:

- *`111122223333`* — El ID de tu AWS cuenta
- *`MyRole`* — La función de IAM que utiliza para administrar AWS Security Agent en la consola
- *`MyApplicationRole`* — El rol de la aplicación creado durante la configuración del AWS Security Agent
- *`us-east-1`* — La AWS región en la que usa AWS Security Agent

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKeyMetadataValidationForApplicationAndAgentSpaces",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyRole"
      },
      "Action": [
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowUseOfHierarchicalKeyringForAgentSpaces",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyRole"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:agent-space":
 "arn:aws:securityagent:us-east-1:111122223333:agent-space/*"
        },
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid": "AllowSynchronousDataAccessForAgentSpaces",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyApplicationRole"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:agent-space":
"arn:aws:securityagent:us-east-1:111122223333:agent-space/*"
        },
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowAsynchronousDataAccessForAgentSpaces",
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:agent-space":
"arn:aws:securityagent:us-east-1:111122223333:agent-space/*"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:securityagent:us-east-1:111122223333:agent-space/*"
        }
      }
    },
    {
```

```
      "Sid": "AllowAsynchronousDataAccessForCodeRemediation",
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Important**
>
> Para rotar las claves de las sucursales, la política de claves de KMS debe conceder `kms:GenerateDataKeyWithoutPlaintext` `kms:ReEncryptFrom` los permisos al director de servicio del AWS Security Agent (`securityagent.amazonaws.com`). De lo contrario, se producirá un error al rotar las claves de la sucursal. `kms:ReEncryptTo` Para obtener más información sobre los permisos necesarios, consulte Rotar una clave de rama.

Política clave para las integraciones

La siguiente política clave otorga a AWS Security Agent los permisos necesarios para cifrar y descifrar los datos de integración, incluidos los resultados de la revisión del código.

Sustituya los siguientes valores de marcador de posición en la política:

- *111122223333* — El ID de tu AWS cuenta
- *MyRole* — La función de IAM que utiliza para administrar AWS Security Agent en la consola
- *us-east-1* — La AWS región en la que usa AWS Security Agent

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

```
      "Principal": {
          "AWS": "arn:aws:iam::111122223333:role/MyRole"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws-crypto-ec:aws:securityagent:integration":
"arn:aws:securityagent:us-east-1:111122223333:integration/*"
        },
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowKeyMetadataValidationForIntegrations",
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "kms:DescribeKey",
      "Resource": "*"
    },
    {
      "Sid": "AllowAsynchronousDataAccessForIntegrations",
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
```

```
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:securityagent:us-east-1:111122223333:integration/*"
        },
        "StringLike": {
          "kms:EncryptionContext:aws-crypto-ec:aws:securityagent:integration":
 "arn:aws:securityagent:us-east-1:111122223333:integration/*"
        }
      }
    }
  ]
}
```

> **Note**
>
> Puede combinar las declaraciones de política clave sobre el espacio de agente, la integración y el paquete de requisitos de seguridad en una sola política clave si desea utilizar la misma clave de KMS para varios tipos de recursos.

Política clave para los paquetes de requisitos de seguridad

La siguiente política de claves otorga a AWS Security Agent los permisos necesarios para cifrar y descifrar los datos del paquete con requisitos de seguridad. Los paquetes de requisitos de seguridad no utilizan una función de aplicación web. La política utiliza dos rutas de acceso:

- Ruta sincrónica: cuando llamas a la API, el servicio usa tus credenciales reenviadas para llamar a AWS KMS en tu nombre (mediante la `kms:ViaService` condición).
- Ruta asíncrona: para las operaciones asincrónicas en las que se pueden usar los paquetes, el servicio utiliza su propio director de servicio para llamar directamente a KMS. AWS

Sustituya los siguientes valores en la política:

- *`111122223333`* — Tu ID AWS de cuenta
- *`MyRole`* — La función de IAM que utiliza para invocar las operaciones del paquete de requisitos de seguridad
- *`us-east-1`* — La AWS región en la que usa Security Agent AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKeyMetadataValidation",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyRole"
      },
      "Action": [
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowUseOfHierarchicalKeyringForSecurityPacks",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyRole"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        },
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:security-requirement-pack":
 "arn:aws:securityagent:us-east-1:111122223333:security-requirement-pack/*"
        }
      }
    },
    {
```

```
      "Sid": "AllowAsynchronousDataAccessForSecurityPacks",
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:security-requirement-pack":
 "arn:aws:securityagent:us-east-1:111122223333:security-requirement-pack/*"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:securityagent:us-east-1:111122223333:security-
requirement-pack/*"
        }
      }
    }
  ]
}
```

La política contiene tres declaraciones:

- AllowKeyMetadataValidation— Se concede `kms:DescribeKey` para que AWS Security Agent pueda validar que la clave gestionada por el cliente existe, está habilitada y utiliza el cifrado simétrico cuando se especifica una CMK durante la creación del recurso. Utiliza la `kms:ViaService` condición para garantizar que la llamada se origine a través del servicio.
- AllowUseOfHierarchicalKeyringForSecurityPacks— Concede `kms:GenerateDataKeyWithoutPlaintext` (crea nuevas claves de bifurcación), `kms:ReEncryptTo` `kms:ReEncryptFrom` (rota las claves de bifurcación existentes) y `kms:Decrypt` (recupera las claves de bifurcación existentes) para operaciones jerárquicas de generación de claves. Estas operaciones utilizan las credenciales reenviadas a través de la ruta sincrónica y se ajustan a los requisitos de seguridad de los recursos del paquete según la condición del contexto de cifrado.
- AllowAsynchronousDataAccessForSecurityPacks— Concede `kms:GenerateDataKeyWithoutPlaintext` `kms:Decryptkms:ReEncryptTo`, y

`kms:ReEncryptFrom` al director de servicio de AWS Security Agent para operaciones asincrónicas cuando no se dispone de las credenciales de la persona que llama.

A diferencia de la política de claves de Agent Spaces, la política del paquete de requisitos de seguridad no incluye el rol principal de una aplicación web. Se accede a los paquetes de requisitos de seguridad a través AWS de la consola de administración mediante su función de administrador, no a través de la aplicación web AWS Security Agent. Todas las operaciones sincrónicas utilizan la función de llamada única (via`kms:ViaService`).

> **Note**
>
> Si utiliza la misma clave KMS tanto para los espacios de agente como para los paquetes de requisitos de seguridad, puede combinar las principales declaraciones de política de ambas secciones en una única política clave.

Política clave para CMK-encrypted AWS recursos

Si proporciona AWS recursos cifrados con una clave administrada por el cliente a AWS Security Agent, debe actualizar la política de claves de la clave KMS de cada recurso para conceder los permisos necesarios. Esto se aplica a los siguientes recursos:

- Depósitos de S3: si proporciona recursos de aprendizaje desde un depósito de S3 cifrado con una clave gestionada por el cliente (SSE-KMS), la política de claves debe permitir que la función de servicio de pruebas de penetración descifre los objetos.
- Secrets Manager Secrets: si tus credenciales de prueba de penetración se almacenan en Secrets Manager secrets cifrados con una clave gestionada por el cliente, la política de claves debe permitir que el rol del servicio de pruebas de penetración descifre esos secretos. Si la aplicación web crea secretos en su nombre, la política de claves también debe permitir que el rol de la aplicación los cifre.
- CloudWatch Grupos de registros: si el grupo de CloudWatch registros utilizado para almacenar los registros de ejecución de las pruebas de intrusión está cifrado con una clave gestionada por el cliente, la política de claves debe permitir a CloudWatch Logs validar la clave de KMS mediante la función de servicio y permitir que el director del servicio de CloudWatch registros realice operaciones criptográficas.

> **Important**
>
> AWS Security Agent también puede crear CloudWatch registros, grupos de registros y secretos de Secrets Manager en su nombre. Al configurar su política de claves de KMS, incluya también las declaraciones correspondientes a estos recursos creados por el servicio.

Las siguientes declaraciones de política clave otorgan los permisos necesarios para CMK-encrypted los recursos. Incluya solo las declaraciones que se apliquen a su configuración. Si un recurso usa la misma clave de KMS que especificó para su espacio de agente, añada estas declaraciones a la política de esa clave. Si un recurso usa una clave de KMS diferente, añada estas declaraciones a la política de esa clave.

Sustituya los siguientes valores de marcador de posición en la política:

- *111122223333* — El ID de tu AWS cuenta
- *MyApplicationRole* — El rol de la aplicación creado durante la configuración AWS del Security Agent
- *MyPenTestServiceRole* — El rol del servicio de pruebas de penetración
- *us-east-1* — La AWS región en la que usas AWS Security Agent

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKmsKeyAccessForCreatingSecrets",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyApplicationRole"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
```

```
        "StringLike": {
          "kms:ViaService": "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:*"
        }
      }
    },
    {
      "Sid": "AllowKmsKeyDecryptionForS3Objects",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyPenTestServiceRole"
      },
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "s3.*.amazonaws.com",
          "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::YOUR-BUCKET-NAME*"
        }
      }
    },
    {
      "Sid": "AllowKmsKeyDecryptionForSecretsManagerSecrets",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyPenTestServiceRole"
      },
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "secretsmanager.*.amazonaws.com",
```

```
          "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:YOUR-SECRET-NAME*"
        }
      }
    },
    {
      "Sid": "AllowKmsKeyValidationForCloudWatchLogsLogGroups",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyPenTestServiceRole"
      },
      "Action": [
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "logs.*.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowKmsKeyAccessForCloudWatchLogsLogGroups",
      "Effect": "Allow",
      "Principal": {
        "Service": "logs.us-east-1.amazonaws.com"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:EncryptionContext:aws:logs:arn": "arn:aws:logs:us-
east-1:111122223333:log-group:YOUR-LOG-GROUP-NAME*"
        }
```

```
      }
    }
  ]
}
```

Note

- La `AllowKmsKeyDecryptionForS3Objects` declaración solo es obligatoria si proporciona recursos de aprendizaje de depósitos de S3 cifrados con una clave administrada por el cliente. Para obtener más información sobre la configuración SSE-KMS de S3, consulte Proteger los datos con SSE-KMS.
- La `AllowKmsKeyDecryptionForSecretsManagerSecrets` declaración solo es necesaria si las credenciales de la prueba de penetración se almacenan en Secrets Manager, secretos cifrados con una clave gestionada por el cliente. El rol de servicio necesita acceso para descifrar los secretos durante las pruebas de penetración. Para obtener más información sobre el cifrado secreto, consulte Cifrado y descifrado secretos en Secrets Manager.
- La `AllowKmsKeyValidationForCloudWatchLogsLogGroups` declaración otorga la función de servicio `kms:DescribeKey` para que CloudWatch Logs pueda validar la clave de KMS a través de la función de servicio al asociarla a un grupo de registros.
- La `AllowKmsKeyAccessForCreatingSecrets` declaración es obligatoria si la aplicación web crea secretos de Secrets Manager en su nombre mediante una clave gestionada por el cliente. El rol de la aplicación `kms:Decrypt` necesita `kms:GenerateDataKey` cifrar el secreto con su clave de KMS.
- La `AllowKmsKeyAccessForCloudWatchLogsLogGroups` declaración otorga al director del servicio de CloudWatch registros (`logs.us-east-1.amazonaws.com`) los permisos que necesita para cifrar y descifrar los datos de registro. Esta declaración también es obligatoria si AWS Security Agent crea un grupo de registros en su nombre cuando usted no proporciona uno existente. Para obtener más información, consulte Cifrar los datos de registro en los CloudWatch registros mediante AWS KMS.
- Si varios recursos comparten la misma clave de KMS, puede combinar las declaraciones en una única política de clave.

Función de administrador

No se requiere ninguna política de IAM adicional para el rol de administrador (el rol de IAM que se usa para administrar AWS Security Agent en la consola).

Rol de la aplicación

Además de la política clave de KMS, asocie la siguiente política de IAM al rol de aplicación especificado durante la configuración del AWS Security Agent. Esta política otorga al rol permisos para usar las claves administradas por el cliente para cifrar y descifrar los datos de Agent Space y crear AWS secretos en Secrets Manager.

Sustituya los siguientes valores de marcador de posición en la política:

- *111122223333* — El ID de tu AWS cuenta
- *us-east-1* — La AWS región en la que usa AWS Security Agent
- Los ARN de la clave de KMS`Resource`: los ARN de las claves de KMS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSynchronousDataAccessForAgentSpaces",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890cd"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333",
          "kms:ViaService": "securityagent.us-east-1.amazonaws.com"
        },
        "StringLike": {
          "kms:EncryptionContext:aws:securityagent:agent-space":
 "arn:aws:securityagent:us-east-1:111122223333:agent-space/*"
        }
```

```
      }
    },
    {
      "Sid": "AllowKmsKeyAccessForCreatingSecrets",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890cd"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:*"
        }
      }
    }
  ]
}
```

> **Note**
>
> La función de aplicación es una función de IAM que se especifica o que la consola crea durante la configuración del AWS Security Agent. La aplicación web asume esta función para recuperar los registros de ejecución de las pruebas de penetración y crear secretos de Secrets Manager en su nombre.
>
> - La `AllowKmsKeyAccessForCreatingSecrets` declaración es obligatoria si configura los recursos de autenticación para las pruebas de penetración y decide introducir las credenciales directamente en lugar de especificar un secreto existente. La aplicación web crea un secreto en su nombre y el rol de la aplicación necesita los permisos de esta declaración para cifrar el secreto con la clave administrada por el cliente especificada

para su espacio de agente. Actualice los `Resource` ARN de esta declaración para que coincidan con la clave de KMS utilizada en su espacio de agente.

Rol de servicio

Durante las pruebas de penetración, AWS Security Agent asume la función de servicio de pruebas de penetración para acceder a sus AWS recursos. Si alguno de estos recursos está cifrado con una clave administrada por el cliente, debe conceder al rol de servicio permisos para usar las claves de KMS correspondientes. Esto se aplica a los siguientes recursos:

- Depósitos de S3: si proporciona recursos de aprendizaje (como documentos de API, modelos de amenazas o código fuente) desde un depósito de S3 cifrado con una clave gestionada por el cliente, el rol de servicio necesita permisos para descifrar los objetos de ese depósito. Para obtener más información sobre la configuración SSE-KMS de S3, consulte Proteger los datos con. SSE-KMS
- Secrets Manager Secrets: si las credenciales de la prueba de penetración se almacenan en Secrets Manager secrets cifrados con una clave gestionada por el cliente, el rol de servicio necesita permisos para descifrar esos secretos. Para obtener más información sobre el cifrado secreto, consulte Cifrado y descifrado secretos en Secrets Manager.
- CloudWatch Grupos de registros: si el grupo de CloudWatch registros utilizado para almacenar los registros de ejecución de las pruebas de penetración está cifrado con una clave gestionada por el cliente (incluidos los grupos de registros creados por AWS Security Agent en su nombre), el rol de servicio necesitará `kms:DescribeKey` permiso para validar la clave. El director del servicio de CloudWatch registros se encarga del cifrado y el descifrado reales de los datos de registro, y esos permisos se conceden mediante la política de claves (consultethe section called “Política de claves”). Para obtener más información sobre el cifrado de los datos de registro, consulte Cifrar los datos de registro en los CloudWatch registros mediante KMS. AWS

> **Important**
>
> Si utiliza para cifrar estos recursos una clave de KMS distinta de la que especificó para su espacio de agente, debe conceder al rol de servicio permisos para cada clave de KMS que proteja un recurso al que acceda el rol de servicio durante las pruebas de penetración.

Adjunte la siguiente política de IAM a la función de servicio de pruebas de penetración. Incluya solo las declaraciones que se apliquen a su configuración.

Sustituya los siguientes valores de marcador de posición en la política:

- *111122223333* — El ID de tu AWS cuenta
- *us-east-1* — La AWS región en la que usa AWS Security Agent
- Los ARN de la clave KMS`Resource`: los ARN de las claves administradas por el cliente que se utilizan para cifrar cada recurso

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKmsAccessForEncryptedS3Buckets",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE-S3-KEY-ID"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "s3.*.amazonaws.com",
          "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::YOUR-BUCKET-NAME*"
        }
      }
    },
    {
      "Sid": "AllowKmsAccessForEncryptedSecrets",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE-SECRETS-KEY-ID"
      ],
```

```
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:YOUR-SECRET-NAME*"
        }
      }
    },
    {
      "Sid": "AllowKmsKeyValidationForCloudWatchLogsLogGroups",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/EXAMPLE-CLOUDWATCH-LOGS-KEY-ID"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "StringLike": {
          "kms:ViaService": "logs.*.amazonaws.com"
        }
      }
    }
  ]
}
```

> **Note**
>
> - La `AllowKmsAccessForEncryptedS3Buckets` declaración solo es obligatoria si proporciona recursos de aprendizaje de depósitos de S3 cifrados con una clave administrada por el cliente. Actualice el `Resource` ARN para que coincida con la clave KMS utilizada para cifrar el depósito de S3 y actualice el `kms:EncryptionContext:aws:s3:arn` valor para que coincida con el nombre del depósito.

- La `AllowKmsAccessForEncryptedSecrets` declaración solo es necesaria si las credenciales de la prueba de penetración se almacenan en Secrets Manager, secretos cifrados con una clave gestionada por el cliente. Actualice el `Resource` ARN para que coincida con la clave KMS utilizada para cifrar sus secretos y actualice el `kms:EncryptionContext:SecretARN` valor para que coincida con su nombre secreto.
- La `AllowKmsKeyValidationForCloudWatchLogsLogGroups` declaración solo es necesaria si su grupo de CloudWatch registros está cifrado con una clave administrada por el cliente, incluidos los grupos de registros creados por AWS Security Agent en su nombre. Actualice el `Resource` ARN para que coincida con la clave KMS utilizada para cifrar el grupo de registros.
- Si varios recursos comparten la misma clave KMS, puede combinar las sentencias y enumerar el ARN de clave compartida una vez en el `Resource` campo.

Cree un recurso con una clave gestionada por el cliente

Puede especificar una clave gestionada por el cliente al configurar AWS Security Agent o al crear recursos individuales. La clave KMS cifra todos los datos que pertenecen a ese recurso y sus subrecursos.

Establezca una clave KMS predeterminada durante la configuración (consola)

Puede configurar una clave KMS predeterminada durante la configuración inicial del AWS Security Agent. Esta clave se usa como predeterminada para los nuevos espacios de agentes y las integraciones, a menos que especifique una clave diferente.

1. En la página Configurar AWS Security Agent, expanda la sección Cifrado (opcional).
2. Seleccione Personalizar la configuración de cifrado (avanzada).
3. En Elija una clave de AWS KMS, seleccione una clave de KMS de su cuenta o introduzca un ARN de clave de KMS.
4. Complete los pasos de configuración restantes y elija Configurar AWS Security Agent.

AWS Security Agent valida la clave KMS para confirmar que existe, está habilitada y utiliza el cifrado simétrico. Si se produce un error en la validación, la configuración no continúa y se recibe un mensaje de error.

Cree un espacio de agente con una clave gestionada por el cliente (consola)

1. En la consola AWS de Security Agent, vaya a la página Agent Spaces.
2. Seleccione Crear espacio de agentes.
3. Introduzca un nombre y una descripción opcional para su espacio de agente.
4. Expanda la sección Avanzado.
5. En Cifrado de datos, elija una de las siguientes opciones:
   - Usar la clave predeterminada de la aplicación: usa la clave KMS predeterminada configurada durante la configuración del AWS Security Agent. Esta opción se selecciona de forma predeterminada si se ha configurado una clave predeterminada.
   - Usar una clave diferente: especifique una clave KMS diferente para este espacio de agentes. Seleccione Personalizar la configuración de cifrado (avanzada) y, a continuación, en Elegir una clave de AWS KMS, seleccione una clave de KMS de su cuenta o introduzca un ARN.
6. Seleccione Crear.

Cree una integración con una clave administrada por el cliente (consola)

1. En la consola AWS de Security Agent, vaya a la página de integraciones.
2. Elija Agregar integración y seleccione su proveedor (por ejemplo, GitHub).
3. Complete el paso 1: instale y autorice la aplicación del proveedor.
4. En el paso 2: registre los detalles, introduzca un nombre de registro y configure los ajustes del proveedor.
5. En la sección Cifrado de datos, seleccione Personalizar la configuración de cifrado (avanzado).
6. En Elija una clave de AWS KMS, seleccione una clave de KMS de su cuenta o introduzca un ARN de clave de KMS.
7. Elija Conectar.

Cree un recurso con una clave administrada por el cliente (AWS (CLI o SDK)

Para especificar una clave administrada por el cliente mediante la AWS CLI o el SDK:

- Incluya el `defaultKmsKeyId` parámetro cuando llame `CreateApplication` para establecer una clave KMS predeterminada para su aplicación. Esta clave se utiliza como alternativa al crear espacios de agente o integraciones sin una clave KMS explícita.

- Incluya el `kmsKeyId` parámetro al llamar `CreateAgentSpace` o `CreateIntegration` cifrar un recurso específico. Esto tiene prioridad sobre el valor predeterminado a nivel de aplicación.

Para obtener información detallada sobre los parámetros, consulte la referencia de la API de AWS Security Agent.

Si no especifica una clave de KMS, AWS Security Agent utilizará la clave de KMS predeterminada a nivel de aplicación, si hay alguna configurada. De lo contrario, el recurso se cifra con claves AWS administradas.

Rotación de claves

AWS Security Agent rota automáticamente las claves de sucursal de forma periódica. La rotación de la clave de bifurcación crea una nueva versión activa de la clave de bifurcación, conservando todas las versiones anteriores. Tras la rotación:

- Los datos nuevos se cifran con la nueva versión de clave de sucursal.
- Los datos cifrados anteriormente se pueden descifrar con la versión anterior de clave de sucursal.
- No es necesario volver a cifrar los datos.

La rotación de claves de sucursal es independiente de la rotación de claves de KMS. Puede activar la rotación automática de claves de KMS para su clave gestionada por el cliente de forma independiente. Para obtener más información, consulte Rotación de claves KMS en la Guía AWS para desarrolladores del Servicio de administración de claves.

Tras la rotación de una clave de bifurcación, hay un breve periodo durante el cual las copias almacenadas en caché de la clave de bifurcación anterior pueden seguir utilizándose para nuevas operaciones de cifrado. Este intervalo viene determinado por el tiempo de vida de la caché interna (TTL) y no afecta a la seguridad de los datos.

Consideraciones

Tenga en cuenta lo siguiente cuando utilice claves administradas por el cliente con AWS Security Agent:

- Las claves administradas por el cliente se aplican únicamente a los recursos nuevos. Los recursos existentes creados antes de configurar una clave administrada por el cliente siguen utilizando el cifrado AWS administrado. No hay migración de los datos existentes.

- Las claves gestionadas por el cliente se especifican en el momento de la creación. La clave KMS se especifica al crear un recurso. No puede agregar ni cambiar la clave KMS de un recurso existente.
- Se admiten varias claves KMS. Puede usar diferentes claves de KMS para diferentes recursos. Por ejemplo, puede usar una clave para los Agent Spaces de producción y otra clave para los Agent Spaces de desarrollo.
- Al deshabilitar o eliminar una clave de KMS, no se puede acceder a los datos. Si deshabilita o programa la eliminación de una clave KMS, AWS Security Agent no podrá descifrar los datos cifrados con esa clave. Los recursos afectados se vuelven inaccesibles hasta que se vuelva a activar la clave. La eliminación de una clave KMS impide permanentemente el acceso a todos los datos cifrados con esa clave.
- Se requieren permisos de política clave. Si elimina los permisos necesarios de su política de claves de KMS, AWS Security Agent no podrá acceder a los datos cifrados. Asegúrese de que la política clave conceda permisos para la función de administrador (utilizada para administrar el servicio en la AWS consola), la función de aplicación (utilizada por la aplicación web), la función de servicio de pruebas de penetración (que asumen los agentes para realizar las pruebas de penetración) y la función principal del servicio de AWS Security Agent, tal como se describe enthe section called “Permisos de KMS necesarios”.
- AWS Se aplican cuotas de KMS. Las operaciones criptográficas realizadas con la clave de KMS se tienen en cuenta para las cuotas de solicitudes de AWS KMS. En condiciones normales de uso, la arquitectura de conjunto de claves jerárquico minimiza las llamadas de KMS mediante el almacenamiento en caché de claves de rama. Para obtener más información, consulte Solicitar cuotas en la Guía para desarrolladores de AWS Key Management Service.

Resolución de problemas

Encuentre soluciones a los errores más frecuentes al utilizar AWS Security Agent.

Acceso denegado: se seleccionó un tipo de GitHub cuenta incorrecto o se especificó un nombre de organización incorrecto

- Instaló la aplicación AWS Security Agent en GitHub la organización deseada, pero configuró incorrectamente el `GitHub Account Type` `User` `Organization`
- Instaló la aplicación AWS Security Agent en la GitHub organización deseada y la `GitHub Account Type` configuró correctamente`Organization`, pero dejó el `Organization Name`

campo en blanco o ingresó un nombre de organización incorrecto que no coincide con la organización en la que instaló la aplicación

Solución:

1. Vaya a la aplicación de la organización GitHub y desinstálela. Para obtener más información, consulte the section called “Paso 1: desinstale la GitHub aplicación AWS Security Agent de GitHub”.
2. Vuelva a la página de integraciones y reinicie el proceso de integración haciendo clic en la aplicaciónAdd `Integrations`, instalándola y autorizándola en la GitHub organización que desee una vez más.
3. Seleccione una opción `Organization` en el menú desplegable de `GitHub account type`
4. Asegúrese de `Organization Name` que la entrada sea EXACTAMENTE la misma en la que instaló la aplicación.
5. Elija Connect para crear la integración de su GitHub organización.

Acceso denegado: permisos insuficientes para instalar GitHub la aplicación en la organización

Cuando intente instalar la aplicación AWS Security Agent en la GitHub organización que desee, verá dos mensajes diferentes en el botón de la página de instalación.

- Una organización `Member` verá `Authorize & Request`
- Una organización `Owner` verá `Install & Authorize`

Para comprobar si es miembro de la GitHub organización `Member` o forma parte `Owner` de ella, siga los pasos que se indican a continuación.

1. Ve a github.com
2. Elige tu perfil en el sitio web
3. Navega hasta `Organizations` el menú desplegable y elígelo
4. Busque la organización en la que desea instalar AWS Security Agent en la lista de organizaciones y especificará si usted es el nombre de la organización `Member` o está `Owner` junto a él.

Posibles soluciones:

- Pida a un propietario que apruebe su solicitud de instalación ANTES de intentar crear la integración
- Pide a un propietario que actualice tu función en la GitHub organización de `Member` a a una `Owner` y reinicie de nuevo el proceso de integración

El agente no puede conectarse al punto final durante una prueba de penetración

Si el agente de la prueba de penetración no puede realizar llamadas a la URL de destino configurada o no puede navegar correctamente por el punto final de destino:

- Si su terminal realiza llamadas a dominios fuera de la URL de destino configurada, compruebe que los dominios adicionales se hayan agregado como URL accesibles en su configuración de pentest
- Actualmente, las pruebas de penetración solo están disponibles para los HTTP/HTTPS puntos finales que atienden el tráfico en los puertos 80 o 443
- Si tiene un WAF configurado, compruebe que el WAF no esté bloqueando el tráfico de las pruebas de penetración. Puede permitir el tráfico de las pruebas de penetración de la lista por `User-Agent` encabezado, que se establecerá de forma predeterminada `securityagent`

Cómo obtener ayuda adicional

Si sigues teniendo problemas después de probar estos pasos de solución de problemas:

- Consulte la página de estado del servicio AWS Security Agent
- Póngase en contacto con AWS Support para obtener ayuda con problemas de configuración complejos

Para usuarios y desarrolladores (aplicación web e IDE)

Realice revisiones del diseño, los modelos de amenazas, las revisiones del código y las pruebas de penetración en la aplicación web, un IDE o un proveedor de fuentes conectado y, a continuación, revise y corrija los hallazgos.

Inicie sesión en la aplicación web AWS Security Agent

Debe iniciar sesión en la aplicación web AWS Security Agent para completar tareas como:

- Realice una revisión del diseño
- Realice una prueba de penetración

Métodos de acceso

AWS Security Agent proporciona diferentes métodos para acceder a la aplicación web, en función de cómo configuró su organización el acceso durante la configuración inicial y de si tiene acceso a la consola de AWS.

Centro de identidad de IAM (SSO): si su organización ha habilitado el Centro de identidades de IAM, puede iniciar sesión con sus credenciales de SSO. Debe tener asignado al menos un espacio de agente en el Centro de identidades de IAM para poder acceder a la aplicación web.

Acceso de administrador (IAM): si tiene acceso a la consola de AWS con los permisos adecuados, puede lanzar la aplicación web a través del enlace de acceso de administrador de cualquier página de Agent Space. Este método proporciona la autenticación a través de su sesión de consola actual.

> **Note**
>
> El método de acceso principal que utiliza su organización se determinó durante la configuración inicial de AWS Security Agent. Para obtener información sobre la configuración del acceso y las asignaciones de los usuarios, consultethe section called “Otorgue a los usuarios acceso a la aplicación web AWS Security Agent”.

Inicie sesión con IAM Identity Center (SSO)

Si su organización configuró el acceso al IAM Identity Center, puede iniciar sesión en la aplicación web con sus credenciales de SSO a través de varios puntos de entrada.

Requisitos previos

- Se le ha asignado al menos un espacio de agente en el Centro de Identidad de IAM
- Tiene sus credenciales de SSO del IAM Identity Center

Acceda a la aplicación web

Elija uno de los siguientes métodos en función de sus necesidades:

Para ver todos los espacios de agentes a los que está asignado:

1. En la consola de AWS Security Agent, vaya a Configuración.
2. Localice el dominio de la aplicación web y copie la URL.

> **Tip**
>
> Marque esta URL como favorita para acceder a ella fácilmente. Este es el punto de entrada universal para ver todos los espacios de agente a los que está asignado.

3. Navegue hasta la URL de la aplicación web.
4. Introduzca sus credenciales del centro de identidad de IAM cuando se le pida.
5. Tras la autenticación, verá una lista de todos los espacios de agente a los que está asignado.
6. Selecciona el espacio de agentes en el que quieres trabajar.

Para acceder directamente a un espacio de agente específico (requiere acceso a la consola AWS):

1. Inicie sesión en la consola de administración de AWS.
2. Navegue hasta la consola de AWS Security Agent.
3. Navegue hasta el espacio de agentes al que desee acceder.
4. Seleccione una de las siguientes opciones:
   - Abra el botón de la aplicación web en la página de información general de Agent Space

- Abre el botón de la aplicación web en la sección de revisión del código
- Abre el botón de la aplicación web en la sección de pruebas de penetración

5. Introduzca sus credenciales del IAM Identity Center cuando se le pida.
6. Tras la autenticación, accederá directamente a ese espacio de agente en la aplicación web.

> **Note**
>
> Si no tiene acceso a la consola de AWS, utilice el dominio de la aplicación web de la página de configuración para acceder a todos los espacios de agente asignados.

Inicie sesión con acceso de administrador (IAM)

Si tiene acceso a la consola de AWS con los permisos de AWS Security Agent adecuados, puede lanzar la aplicación web a través del enlace de acceso de administrador con autenticación automática.

Requisitos previos

- Ha iniciado sesión en la consola de administración de AWS
- Dispone de los permisos adecuados para acceder a los recursos de AWS Security Agent

Acceda a la aplicación web

Elija uno de los siguientes métodos:

Para acceder a un espacio de agente específico:

1. Inicie sesión en la consola de administración de AWS.
2. Navegue hasta la consola de AWS Security Agent.
3. Navegue hasta el espacio de agentes al que desee acceder.
4. Pulse el botón de acceso de administrador en la página de información general del espacio de agentes.
5. La aplicación web se abre en una nueva pestaña con autenticación automática para ese espacio de agente.

> **Note**
>
> El botón de acceso de administrador siempre está disponible para los usuarios con acceso a la consola de AWS, independientemente de si su organización utiliza el Centro de identidades de IAM como método de acceso principal.

Crear una revisión de diseño

Compare sus documentos de diseño con los requisitos de seguridad de la organización cargando archivos para que AWS Security Agent los revise. Las revisiones del diseño ayudan a identificar los problemas de seguridad al principio del ciclo de vida del desarrollo, lo que le permite abordar los problemas de arquitectura cuando resulta más rentable resolverlos.

AWS Security Agent analiza sus documentos de diseño para compararlos con los requisitos de seguridad de su organización y proporciona resultados de seguridad detallados para mejorar la postura de seguridad antes de que comience la implementación.

En este procedimiento, creará una revisión del diseño cargando archivos de diseño para su análisis.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Acceso a la aplicación web AWS Security Agent
- Diseñe documentos listos para su carga (DOC, DOCX, JPEG, MD, PDF, PNG y TXT)
- Cada archivo debe tener 2 MB o menos, con un total combinado de 6 MB en todos los archivos
- Comprenda qué requisitos de seguridad están habilitados para su organización

Paso 1: Comience a crear una revisión del diseño

Navegue hasta la página de creación de la revisión de diseño en la aplicación web Agent.

1. Inicie sesión en la aplicación web AWS Security Agent.
2. Diríjase a la sección de revisiones de diseño.
3. Seleccione Crear revisión de diseño.

> **Tip**
>
> Para ver los requisitos de seguridad habilitados por su organización, vaya a la página de requisitos de seguridad de la consola de AWS Security Agent. Seleccione cualquier requisito habilitado para ver sus detalles. Estos requisitos se utilizan para analizar los archivos de diseño.

Paso 2: Asigne un nombre a la revisión del diseño

Proporcione un nombre descriptivo que ayude a identificar el propósito y el alcance de esta revisión del diseño.

1. En la sección Nombre de la revisión del diseño, localice el campo Nombre.
2. Introduzca un nombre descriptivo para la revisión del diseño.

> **Note**
>
> El nombre debe identificar claramente el proyecto, la función o el componente que se está revisando. 80 caracteres como máximo.

Paso 3: Sube los archivos de diseño

Cargue los documentos de diseño que desee que AWS Security Agent analice para comprobar el cumplimiento de las normas de seguridad.

1. En la sección Archivos para revisar, revise los requisitos del archivo:

> **Important**
>
> Se puede cargar un máximo de 5 archivos por revisión de diseño. Cada archivo debe tener 2 MB o menos, con un total combinado de 6 MB en todos los archivos. Formatos compatibles: DOC, DOCX, JPEG, MD, PDF, PNG y TXT.

2. Cargue sus archivos mediante uno de estos métodos:
   a. Arrastrar y soltar: arrastra los archivos directamente al área de la zona de entrega de archivos
   b. Explorar: usa el botón Elegir archivos para buscar y seleccionar archivos de tu computadora

3. Compruebe que se hayan cargado todos los archivos necesarios.

> **Tip**
>
> Para obtener los mejores resultados, incluya diagramas de arquitectura, especificaciones de diseño y documentación técnica que describan los componentes y flujos de datos relevantes para la seguridad del sistema.

Paso 4: Iniciar la revisión del diseño

Tras configurar toda la información requerida, inicie el análisis de seguridad de los documentos de diseño.

1. Revise todos los archivos y ajustes cargados para garantizar su precisión.
2. Selecciona Iniciar la revisión del diseño.
3. AWS Security Agent analiza sus documentos de diseño comparándolos con los requisitos de seguridad habilitados.

> **Note**
>
> El proceso de revisión del diseño normalmente se completa en cuestión de minutos, en función de la cantidad y el tamaño de los archivos cargados. Recibirá las conclusiones de seguridad en función de los requisitos de seguridad de su organización.

Siguientes pasos

Tras iniciar la revisión del diseño:

- Supervise el progreso de la revisión en la aplicación Agent Web
- Revise los resultados de seguridad.
- Comparta las conclusiones con su equipo de desarrollo
- Aborde los hallazgos de seguridad identificados en su diseño
- Actualice los documentos de diseño y vuelva a enviarlos si es necesario

Revise los resultados de una revisión de diseño

Los resultados de la revisión le ayudan a comprender qué requisitos de seguridad se cumplen, cuáles requieren atención y qué medidas debe tomar para mejorar la postura de seguridad de su diseño antes de que comience la implementación.

En este procedimiento, aprenderá a acceder a los resultados de la revisión del diseño, filtrarlos e interpretarlos para abordarlos de manera eficaz.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Una revisión de diseño completa
- Acceso a la aplicación web AWS Security Agent
- Familiaridad con los requisitos de seguridad habilitados por su organización

Paso 1: Acceda a la revisión del diseño

Navegue hasta la revisión de su diseño para ver los hallazgos y la información resumida.

1. Inicie sesión en la aplicación web AWS Security Agent.
2. Navegue hasta la sección de revisiones de diseño.
3. Seleccione de la lista la revisión de diseño que desee examinar.

> **Tip**
>
> La página de detalles de la revisión del diseño muestra un resumen del estado de la revisión, la fecha de finalización y el número de archivos revisados.

Paso 2: Revise el resumen de las conclusiones

Examine el resumen de alto nivel para comprender la postura general de seguridad de su diseño.

1. Localice la sección de resumen.
2. Revise el recuento de cada categoría de estado de cumplimiento: conforme Non-compliant, datos insuficientes y no aplicable.

> **Note**
>
> El resumen proporciona los recuentos para cada tipo de estado, lo que le ayuda a evaluar rápidamente el número de hallazgos que requieren atención. Para obtener una explicación detallada de cada estado, consulte el paso 4.

Paso 3: Filtrar y explorar los hallazgos

Utilice las funciones de filtrado y búsqueda para centrarse en hallazgos o estados de cumplimiento específicos.

1. En la sección Revisar los resultados, localice los controles del filtro.
2. Para filtrar por estado:
   a. Selecciona el menú desplegable de estado.
   b. Seleccione un estado de cumplimiento específico para ver solo los hallazgos con ese estado.
3. Para buscar requisitos de seguridad específicos:
   a. Introduzca las palabras clave en el campo de búsqueda.
   b. Los resultados se actualizan automáticamente a medida que escribes.
4. Utilice los controles de paginación para navegar por varias páginas de resultados.

> **Tip**
>
> Filtre primero por Non-compliantestado para priorizar los hallazgos que requieren atención inmediata en su diseño.

Paso 4: Comprenda los estados de cumplimiento

Cada resultado muestra un estado de conformidad que indica cómo su diseño aborda un requisito de seguridad específico:

- Conforme: su diseño cumple con los requisitos de seguridad según el análisis
- Non-compliant— Su diseño infringe o aborda de manera inadecuada el requisito de seguridad
- Datos insuficientes: los archivos cargados carecen de información suficiente para determinar el cumplimiento

- No aplicable: el requisito de seguridad no se aplica al diseño del sistema

> **Important**
>
> Concéntrese en los estados de datos Non-compliante insuficientes, ya que requieren una acción. Aborde los casos de incumplimiento actualizando su diseño y resuelva los hallazgos de datos insuficientes cargando documentación de diseño adicional.

Paso 5: Ver los detalles de la búsqueda

Seleccione los hallazgos individuales para ver una guía detallada de justificación y remediación.

1. En la tabla de resultados, seleccione el nombre de un requisito de seguridad.
2. Revise los detalles del hallazgo, que incluyen:
   - El requisito de seguridad específico que se está evaluando
   - Un comentario que explique por qué el hallazgo recibió su estado de conformidad, incluyendo detalles específicos sobre lo que falta o no es conforme
   - Guía de corrección recomendada para abordar el hallazgo
   - Enlaces a la documentación interna de su organización o a las normas sobre los requisitos de seguridad

> **Note**
>
> El comentario explica el razonamiento de AWS Security Agent con detalles específicos. Si los datos encontrados son insuficientes, el comentario identifica qué información falta, por ejemplo: «Los documentos de diseño no mencionan los mecanismos de autenticación» o «No se ha encontrado información sobre el cifrado de datos en reposo».

Paso 6: Abordar las conclusiones

Tome medidas en función de los hallazgos que requieran atención para mejorar la postura de seguridad de su diseño.

Para ver Non-compliantlas conclusiones:

1. Revise la guía de remediación recomendada.
2. Revise cualquier documentación interna vinculada para obtener más información sobre el contexto.
3. Actualice sus documentos de diseño para cumplir con los requisitos de seguridad.
4. Documente los cambios que realice para consultarlos en el futuro.

En caso de encontrar datos insuficientes:

1. Lee el comentario detenidamente para entender qué información específica falta.
2. Cree o actualice documentos de diseño con los detalles que faltan.
3. Prepare los archivos actualizados para volver a enviarlos.

Siguientes pasos

Tras revisar los resultados del diseño:

- Descarga el informe de resultados en un archivo CSV para compartirlo con tu equipo
- Actualice los documentos de diseño para abordar los hallazgos no conformes
- Cree documentación adicional para detectar datos insuficientes
- Comparta los resultados con su equipo de desarrollo para debatirlos
- Clone esta revisión de diseño para crear una nueva revisión con los documentos originales precargados, lo que le permitirá actualizar el nombre y volver a ejecutar el análisis para comprobar las mejoras
- Continúe con la implementación de los diseños que cumplan con los requisitos de conformidad

Para obtener más información sobre la gestión de los requisitos de seguridad, consultethe section called “Gestione los requisitos de seguridad”.

Para obtener más información sobre la creación de revisiones de diseño, consultethe section called “Crear una revisión de diseño”.

Cree un modelo de amenazas

Cree modelos de amenazas en la aplicación web AWS Security Agent para analizar la arquitectura de la aplicación e identificar las amenazas de seguridad. Un modelo de amenazas produce dos

resultados principales: una descripción general del sistema que describe cómo está construido y cómo se comporta el sistema, y un conjunto de amenazas que describen cómo se podría atacar el sistema, cada una con un nivel de gravedad, una clasificación STRIDE y recomendaciones prácticas.

Un modelo de amenazas acepta dos tipos de entradas y puedes proporcionar una de ellas o ambas:

- Documentos de alcance: documentos de diseño técnico, especificaciones de API o documentación de arquitectura que definen en qué se centra el modelo de amenazas. Cuando se proporcionan, el agente limita su análisis al contexto descrito en estos documentos. Puedes cargar archivos (DOC, DOCX, JPEG, MD, PDF, PNG, TXT), proporcionar URI de S3 o conectar páginas de Confluence mediante una integración.
- Fuentes: código fuente de los repositorios conectados (GitHub GitHub Enterprise Server o Bitbucket) o de ubicaciones de S3. GitLab GitLab Self-Managed AWS Security Agent lee el código fuente para comprender su sistema actual. Cuando se combina con los documentos de alcance, el código fuente proporciona un contexto sobre la implementación actual.

En este procedimiento, se crea un modelo de amenazas configurando sus entradas y permisos y, a continuación, se inicia una ejecución.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Acceso a la aplicación web AWS Security Agent
- Al menos una de las siguientes opciones:
  - Un repositorio conectado (GitHub GitHub Enterprise Server o Bitbucket) para usarlo como fuente (consultethe section called “Habilitar el modelado de amenazas”) GitLab GitLab Self-Managed
  - Un bucket de S3 que contiene el código fuente
  - Diseña documentos para subirlos como documentos de alcance o como una integración de Confluence

> **Tip**
>
> Si ya tienes repositorios o depósitos de S3 conectados a tu Agent Space (por ejemplo, mediante una configuración de revisión de código o pruebas de penetración), puedes crear

un modelo de amenazas de forma inmediata, sin necesidad de realizar ninguna configuración adicional.

Cómo AWS Security Agent ejecuta un modelo de amenazas

Las entradas que proporcione determinan cómo AWS Security Agent ejecuta el modelo de amenazas. Existen tres escenarios.

Entradas que usted proporciona	Cómo ejecuta AWS Security Agent el modelo de amenazas
Solo fuentes (código fuente)	AWS Security Agent analiza el código fuente para comprender la estructura de la aplicación, clasifica los componentes, extrae los flujos de datos, crea un modelo de amenazas e identifica las amenazas en función de cómo se implementa realmente el sistema.
Solo documentos de alcance (documentos de diseño)	AWS Security Agent ejecuta un modelo de amenazas centrado en el diseño descrito en sus documentos. Identifica las amenazas en función de la arquitectura, los flujos de datos y los componentes descritos en los documentos de alcance, lo que resulta útil para modelar las amenazas de un diseño antes de que exista el código.
Tanto las fuentes como los documentos de alcance	AWS Security Agent limita el modelo de amenazas al contexto descrito en los documentos de alcance (por ejemplo, un documento de diseño para una nueva función). Utiliza el código fuente para comprender su sistema actual y, a continuación, modela las amenazas según el diseño descrito en los documentos de alcance, independientemente de que el diseño ya esté implementado o no.

Acceda a la página de modelos de amenazas

Navegue hasta la sección de modelado de amenazas en la aplicación web.

1. Inicie sesión en la aplicación web AWS Security Agent.
2. En la barra lateral izquierda, selecciona Modelos de amenazas.

3. Verá una lista de los modelos de amenazas existentes con su título, estado de última ejecución y recuentos de amenazas por gravedad.

Cree un modelo de amenazas

Configure un nuevo modelo de amenazas configurando sus entradas y permisos.

1. En la página Modelos de amenazas, elija Crear modelo de amenazas.

Configure los detalles del modelo de amenazas

Proporcione un título para su modelo de amenazas.

1. En el campo Título, introduzca un nombre descriptivo para su modelo de amenazas.

> **Tip**
>
> Utilice un nombre que identifique la aplicación o el servicio que se está modelando. Por ejemplo, «billing-service» o «checkout-api».

Agregue documentos de alcance

Proporcione los documentos de diseño técnico que definan en qué se centra el modelo de amenazas, como la documentación de arquitectura, las especificaciones de la API o las propuestas de diseño. Cuando se proporcionan los documentos de alcance, el agente limita su análisis al contexto descrito en estos documentos. Los documentos de alcance son opcionales si se proporcionan las fuentes.

1. En la sección Documentos de ámbito, añade documentos mediante uno o varios de los métodos siguientes:
   - Cargue archivos: cargue los documentos de diseño directamente (DOC, DOCX, JPEG, MD, PDF, PNG o TXT).
   - URI de S3: introduzca los URI de S3 que apunten a los documentos almacenados en los depósitos S3 conectados.
   - Páginas de Confluence: si tienes una integración de Confluence conectada a tu espacio de agente, selecciona las páginas de tu espacio de trabajo de Confluence.

> **Tip**
>
> Para obtener los mejores resultados, incluye diagramas de arquitectura, especificaciones de API y documentación técnica que describa los componentes, los flujos de datos y los límites de confianza del sistema.

Añada fuentes

Seleccione el código fuente que usa AWS Security Agent para comprender su sistema actual. Cuando se combina con los documentos de alcance, el código fuente proporciona un contexto sobre la implementación actual: el agente lo usa para entender lo que ya existe. Las fuentes son opcionales si se proporcionan los documentos de alcance.

1. En la sección Fuentes, añade el código fuente mediante uno o varios de los métodos siguientes:

Repositorios integrados

Seleccione uno de los repositorios conectados a su espacio de agente (GitHub GitHub Enterprise Server o GitLab Self-Managed Bitbucket). GitLab

1. Selecciona la casilla de verificación situada junto a cada repositorio que quieras incluir como fuente.
2. Usa el campo de búsqueda para buscar repositorios específicos por nombre.

> **Note**
>
> Aquí solo aparecen los repositorios conectados a su espacio de agente. Para añadir más repositorios, pida a su administrador que actualice la configuración de Agent Space.

Orígenes de S3

Añada los URI de S3 que apunten al código fuente almacenado en los buckets S3 conectados.

1. Introduzca el URI de S3 para cada ubicación del código fuente que desee incluir.

Configurar los recursos de AWS

Seleccione la función de servicio de IAM y el grupo de CloudWatch registros opcional para este modelo de amenazas.

1. En el menú desplegable del rol de servicio, seleccione el rol de IAM entre los roles de servicio configurados.

> **Note**
>
> El rol de servicio debe tener permisos para acceder al código fuente en S3 y escribir CloudWatch en los registros. Las funciones de servicio se configuran durante la configuración de Agent Space en la consola de administración de AWS.

2. (Opcional) En el menú desplegable de grupos de registros, seleccione un grupo de CloudWatch registros para almacenar los registros de ejecución del modelo de amenazas.

Cree el modelo de amenazas

1. Revisión de la configuración de seguridad de .
2. Elija Crear modelo de amenazas.

Se le redirigirá a la página de detalles del modelo de amenazas, donde podrá iniciar una ejecución.

Ejecute un modelo de amenazas

Tras crear un modelo de amenazas, inicie una ejecución para iniciar el análisis.

1. En la página de detalles del modelo de amenazas, seleccione Iniciar ejecución.
2. AWS Security Agent comienza a analizar sus fuentes y documentos de alcance.

También puede iniciar una ejecución desde la página de lista de modelos de amenazas seleccionando Iniciar ejecución junto al modelo de amenaza que desee ejecutar.

Supervise la ejecución de un modelo de amenazas

Realice un seguimiento del progreso de su modelo de amenazas a medida que se ejecuta.

Estado de ejecución

El encabezado de la página de ejecución muestra un indicador de estado:

- En curso: el agente del modelo de amenazas se está ejecutando.
- Detención: se solicitó una cancelación; el agente está finalizando su tarea actual antes de detenerla.
- Completada: la ejecución finalizó correctamente.
- Falló: se produjo un error en la ejecución. Aparece un mensaje de error con detalles. Inicie una nueva ejecución después de resolver el problema.
- Detenida: el usuario canceló la ejecución. Se conservan todas las amenazas generadas antes de la parada.

Ejecute pestañas de página

En la página de detalles de la ejecución, navega entre las pestañas:

- Descripción general: consulte el resumen de la ejecución (identificador del trabajo, hora de inicio, estado y duración) con un gráfico circular de niveles de gravedad que muestre el desglose de las amenazas por gravedad (crítica, alta, media o baja). Debajo del resumen, consulta un gráfico de barras de las categorías de amenazas de STRIDE que muestra el número de amenazas incluidas en cada categoría de STRIDE. Una vez finalizada la ejecución, consulta la descripción general del sistema elaborada por el agente.
- Configuración: vea las fuentes, los documentos y los permisos (función de servicio, grupo de CloudWatch registro) que se utilizaron para esta ejecución.
- Verificación previa: consulte el estado de las comprobaciones previas que se ejecutan antes de que comience el análisis de amenazas, incluida la configuración de la infraestructura de registro, la validación del acceso a la fuente S3 (cuando corresponda) y la configuración del entorno de prueba. Una barra de progreso muestra cuántas comprobaciones se han completado.
- Registros: permite ver una lista filtrable de las tareas que el agente realizó durante la ejecución. Seleccione cualquier tarea para ver su salida de registro detallada en un panel lateral.
- Amenazas: vea las amenazas identificadas durante la ejecución (consultethe section called “Revise las amenazas a partir de un modelo de amenazas”).

Historial de ejecuciones

Cada modelo de amenazas mantiene un historial de todas las ejecuciones. En la página de detalles del modelo de amenazas:

- La tabla de ejecuciones muestra todas las ejecuciones con su hora de inicio, estado, duración, recuento de amenazas e identificador.
- Selecciona el enlace de la hora de inicio de cualquier ejecución para ver todos sus detalles.

> **Tip**
>
> Re-run el mismo modelo de amenazas después de actualizar el código fuente o revisar los documentos de alcance para ver cómo cambian la descripción general del sistema y las amenazas a lo largo del tiempo.

Edite un modelo de amenazas

Para modificar la configuración del modelo de amenazas:

1. En la página de detalles del modelo de amenazas, seleccione Editar.
2. Actualice el título, las fuentes, los documentos de alcance o los recursos de AWS según sea necesario.
3. Seleccione Save changes (Guardar cambios).

> **Note**
>
> La edición de un modelo de amenazas no afecta a las ejecuciones completadas anteriormente. Conservan la instantánea de configuración utilizada en el momento en que se ejecutaron.

Eliminar un modelo de amenazas

Para eliminar un modelo de amenazas y todas sus ejecuciones y amenazas asociadas:

1. En la página de detalles del modelo de amenazas, abra el menú de acciones y seleccione Eliminar.
2. Confirme la eliminación.

> **Important**
>
> Si hay una ejecución en curso, debe detenerla antes de eliminar el modelo de amenazas.

Siguientes pasos

Tras ejecutar un modelo de amenazas:

- Revise la descripción general del sistema y las amenazas (consultethe section called “Revise las amenazas a partir de un modelo de amenazas”)
- Re-run el modelo de amenazas tras realizar cambios para comprobar que se han abordado las amenazas
- Ajusta tus fuentes y documentos de alcance a medida que tu aplicación evoluciona

Revise las amenazas a partir de un modelo de amenazas

Una vez finalizada la ejecución de un modelo de amenazas, revise la descripción general del sistema y las amenazas para comprender cómo se podría atacar su aplicación y qué hacer al respecto. La descripción general del sistema es un documento completo que describe la arquitectura, los límites de confianza, los flujos de datos y el nivel de seguridad de la aplicación. Cada amenaza incluye una declaración, un nivel de gravedad, una clasificación STRIDE, los activos afectados y una recomendación para abordarla.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Ejecución de un modelo de amenazas completo
- Acceso a la aplicación web AWS Security Agent

Paso 1: Acceda al modelo de amenazas y ejecute

Navegue hasta la ejecución completa del modelo de amenazas.

1. Inicie sesión en la aplicación web AWS Security Agent.
2. En la barra lateral izquierda, selecciona Modelos de amenazas.
3. Seleccione el modelo de amenaza que desee examinar.
4. En la tabla de ejecuciones, seleccione la ejecución completada eligiendo su enlace de hora de inicio.

Paso 2: Revise la descripción general del sistema

La descripción general del sistema es una descripción completa de cómo AWS Security Agent entiende su sistema. Se trata de un documento estructurado que puede incluir:

- Propósito: qué hace el sistema y a quién sirve.
- Capacidades: funcionalidad clave que proporciona el sistema.
- Intención del diseño: el cambio de diseño o la característica que se está modelando como amenaza (cuando se proporcionan los documentos de alcance).
- Arquitectura: cómo se construye el sistema, incluidos los patrones de implementación y los protocolos de comunicación.
- Componentes: una tabla de los componentes del sistema con su propósito e interacciones clave.
- Límites de confianza: dónde cambian los contextos de seguridad, incluidas las protecciones que existen en cada cruce.
- Flujos de datos: descripciones detalladas de cómo se mueven los datos por el sistema, incluidos los protocolos, las credenciales y las protecciones en cada paso.
- Postura de seguridad: mecanismos actuales de autenticación, cifrado y control de acceso.
- Activos confidenciales: datos y credenciales que requieren protección, con sus puntos de clasificación y exposición.
- Suposiciones clave: Security-relevant suposiciones que el agente hizo sobre el sistema.

Para revisar la descripción general del sistema:

1. Seleccione la pestaña Descripción general.

2. Revise la sección de resumen de la ejecución, que muestra el ID del trabajo, la hora de inicio, el estado y la duración.
3. Revise el gráfico de niveles de gravedad, que muestra un desglose de las amenazas por gravedad (crítica, alta, media o baja) con recuentos y porcentajes.
4. Revisa el gráfico de categorías de amenazas, que muestra cuántas amenazas se incluyen en cada categoría de STRIDE (suplantación de identidad, manipulación, repudio, divulgación de información, denegación de servicio, aumento de privilegios).
5. En la sección de descripción general del sistema, lee el análisis completo del agente.

> **Tip**
>
> Si la descripción general del sistema no refleja con precisión su sistema, ajuste sus datos (añada los repositorios relevantes como fuentes o cargue documentos de alcance más completos) y vuelva a ejecutar el modelo de amenazas.

Paso 3: Revise las amenazas

Vaya a la pestaña Amenazas para ver todas las amenazas identificadas durante la ejecución.

1. Seleccione la pestaña Amenazas.
2. Las amenazas se muestran como una lista con cada tarjeta con el título de la amenaza, el indicador de gravedad, el estado y la fecha de la última actualización. Puede filtrar las amenazas por gravedad, estado o buscar por título.
3. Seleccione una amenaza de la lista para ver todos sus detalles en el panel derecho.

Gravedad de la amenaza

A cada amenaza se le asigna un nivel de gravedad:

- Crítico: requiere una acción inmediata; su explotación podría comprometer totalmente el sistema.
- Alto: requiere atención inmediata; la explotación podría tener un impacto significativo en la seguridad.
- Medio: debe abordarse en un plazo razonable; contribuye al riesgo general de seguridad.
- Bajo: se puede abordar como parte de un mantenimiento regular; el riesgo inmediato es mínimo.

Detalles de la amenaza

Seleccione una amenaza para ver sus detalles en el panel derecho. Los detalles se organizan en las siguientes secciones:

Fila de metadatos:

- Gravedad: el nivel de riesgo asignado por el agente (crítico, alto, medio o bajo).
- Categorías STRIDE: la clasificación de amenazas: suplantación de identidad, manipulación, repudio, divulgación de información, denegación de servicio o elevación de privilegios.
- Creado en: cuando se identificó la amenaza.
- Última actualización: fecha en que se modificó la amenaza por última vez.

Sección de descripción:

- Declaración: descripción en lenguaje natural de la amenaza: qué puede hacer la fuente de la amenaza, cuál es el impacto y qué condiciones lo posibilitan.
- Fuente: el actor o el origen de la amenaza (por ejemplo, «usuario autenticado» o «atacante externo»).
- Acción: qué puede hacer la fuente de la amenaza (por ejemplo, «insertar consultas SQL en el parámetro de búsqueda»).
- Impacto: consecuencia directa de la acción de amenaza (por ejemplo, «acceso no autorizado a los registros de los clientes»).

Sección de referencias:

- Activos afectados: activos específicos afectados por la amenaza (por ejemplo, «registros de pagos de clientes» o «tabla de DynamoDB»).
- Requisitos previos: condiciones que deben cumplirse para que la amenaza sea aprovechable.
- Objetivos afectados: objetivos de seguridad afectados: confidencialidad, integridad, disponibilidad, autorización, autenticación o Non-repudiation
- Evidencia: rutas de archivos de código fuente que respaldan la amenaza y que enlazan con archivos específicos de su repositorio.
- Anchor: una referencia de código que vincula la amenaza con un nodo específico del código fuente.

Sección de recomendaciones:

- Recomendación: guía práctica para abordar la amenaza.

Paso 4: Cree una amenaza manualmente

Puede añadir amenazas que el agente no haya identificado, por ejemplo, amenazas descubiertas durante una revisión manual o procedentes de fuentes externas.

1. En la pestaña Amenazas de una ejecución finalizada, seleccione Crear amenaza.
2. Complete los detalles de la amenaza:
   - Declaración: descripción en lenguaje natural de la amenaza.
   - Gravedad: seleccione Crítico, Alto, Medio o Bajo.
   - Fuente: el actor o el origen de la amenaza.
   - Requisitos previos: condiciones necesarias para que la amenaza sea explotable.
   - Acción: qué puede hacer la fuente de la amenaza.
   - Impacto: consecuencia directa de la acción de amenaza.
   - Activos afectados: activos específicos afectados (separados por comas).
   - Objetivos de seguridad afectados: seleccione entre confidencialidad, integridad, disponibilidad, autorización, autenticación o. Non-repudiation
   - Categorías STRIDE: selecciona las categorías aplicables.
   - Recomendación: guía para abordar la amenaza.
3. Seleccione Crear.

La amenaza creada manualmente aparece en la lista de amenazas junto con las amenazas generadas por los agentes.

Paso 5: Editar y clasificar las amenazas

A medida que revisa las amenazas, puede editar sus detalles y actualizar su estado para hacer un seguimiento de su progreso.

1. Seleccione una amenaza de la lista.
2. Seleccione el icono de edición en el panel de detalles de la amenaza para abrir el formulario de edición.

3. Puede modificar los siguientes campos:
   - Estado: realice un seguimiento del ciclo de vida de las amenazas:
     - Abierta: la amenaza se reconoce y requiere atención (opción predeterminada).
     - Resuelto: has solucionado el problema.
     - Rechazado: revisó la amenaza y determinó que no era aplicable.
   - Gravedad: ajuste el nivel de gravedad si la evaluación del agente no coincide con su contexto.
   - Declaración: refine la descripción de la amenaza.
   - Origen, requisitos previos, acción e impacto: actualice los detalles de la amenaza en función de sus conocimientos del dominio.
   - Activos afectados: añada o elimine los activos afectados (separados por comas).
   - Objetivos de seguridad afectados: seleccione los objetivos de seguridad afectados (confidencialidad, integridad, disponibilidad, autorización, Non-repudiation autenticación).
4. Seleccione Guardar para aplicar los cambios.

Paso 6: Descargar un informe

Una vez finalizada la ejecución, puede descargar un informe en PDF que resume la descripción general del sistema y todas las amenazas identificadas.

1. En la página de ejecución completa, seleccione Generar informe.
2. El PDF se descarga en su ordenador.

Paso 7: Revise las comprobaciones y los registros previos a la verificación

Si necesita investigar cómo llegó el agente a sus conclusiones o depurar un error parcial:

1. Seleccione la pestaña Verificación previa para ver el estado de las comprobaciones previas a la verificación que se ejecutan antes de que comience el análisis de amenazas. Cada comprobación muestra su estado (completa, en curso o pendiente) y una barra de progreso indica cuántas comprobaciones se han completado. Puede ampliar una comprobación completada para ver su salida de registro detallada.
2. Seleccione la pestaña Registros para ver una lista filtrable de las tareas que el agente realizó durante la ejecución. Seleccione cualquier tarea de la lista para ver su salida de registro detallada en el panel lateral.

Siguientes pasos

Tras revisar los resultados del modelo de amenazas:

- Aborde primero las amenazas de alta gravedad según las recomendaciones del agente
- Actualice los estados de las amenazas a medida que implemente las correcciones
- Ejecute un nuevo modelo de amenazas para comprobar que los cambios abordan las amenazas identificadas
- Ajuste las fuentes y los documentos de alcance a medida que la aplicación evolucione (consultethe section called “Cree un modelo de amenazas”)

Revisa los hallazgos de seguridad del código en las solicitudes de cambios

Tras habilitar la revisión del código de las solicitudes de extracción para sus repositorios, AWS Security Agent analiza automáticamente las solicitudes de extracción y publica los hallazgos de seguridad directamente en su proveedor de control de código fuente. Esto permite a los desarrolladores abordar los problemas de seguridad dentro de su flujo de trabajo normal sin abandonar la solicitud de extracción de información.

> **Note**
>
> Esta página se aplica a las solicitudes de GitHub extracción, las solicitudes de GitLab fusión y las solicitudes de extracción de Bitbucket. La experiencia es similar en todos los proveedores.

Cómo funciona la revisión del código en las solicitudes de incorporación de cambios

Cuando envías una solicitud de extracción (o una solicitud de fusión GitLab) en un repositorio con la revisión de código habilitada, AWS Security Agent comienza el análisis automáticamente.

1. Activación del análisis de las solicitudes de extracción: la revisión del código se activa cuando una solicitud de extracción se marca como «Lista para su revisión» en los repositorios en los que se

ha activado la función de revisión de código. Los borradores de solicitudes de extracción no se analizan.

2. Reconocimiento del análisis: cuando AWS Security Agent comienza a analizar tu solicitud de cambios, publica un comentario inicial: «El agente de seguridad de AWS está analizando tu código...». Esto te permite saber que el análisis se ha iniciado y está en curso.
3. Finalización de la revisión: una vez finalizado el análisis, AWS Security Agent publica una revisión en tu solicitud de extracción con los resultados. Todos los resultados de seguridad se agrupan en una sola revisión para mantener la solicitud de extracción de información organizada y minimizar las notificaciones.

Comprender los resultados de la revisión del código

AWS Security Agent proporciona distintos tipos de resultados en función de lo que encuentre durante el análisis.

Cuando se detectan problemas de seguridad

Si AWS Security Agent identifica problemas de seguridad en sus cambios de código, publica una reseña que incluye:

- Resumen: una descripción general de alto nivel de todos los hallazgos de seguridad, que describe los tipos de problemas identificados y su posible impacto
- Hallazgos individuales: los hallazgos de seguridad detallados aparecen como comentarios agrupados en la revisión principal, y cada uno de ellos incluye:
  - Descripción del problema de seguridad
  - Ubicación del código en la que se detectó el problema
  - Guía de corrección en la que se explica cómo abordar el problema
  - El contexto relevante se basa en la configuración de revisión del código (infracciones de los requisitos de seguridad, vulnerabilidades comunes o ambas)

> **Note**
>
> Los tipos de problemas de seguridad analizados dependen de la configuración de revisión del código. Si configuraste la validación de los requisitos de seguridad, los resultados se referirán a los requisitos de seguridad personalizados de tu organización. Si configuró los

resultados de las vulnerabilidades de seguridad, estos identificarán las vulnerabilidades de seguridad más comunes. Para obtener más información sobre la configuración de revisión de código, consultethe section called “Habilitar la revisión del código de las solicitudes de extracción para los GitHub repositorios”.

Cuando no se detecte ningún problema de seguridad

Si AWS Security Agent completa el análisis y no encuentra ningún problema de seguridad en los cambios de código, publica un comentario: «No se ha identificado ningún problema». Esto confirma que la revisión se ha realizado correctamente y que los cambios en el código no han provocado ningún problema de seguridad en función de los ajustes de revisión de código configurados.

Responder a los hallazgos de seguridad

Tras revisar las conclusiones de seguridad publicadas por AWS Security Agent, puede tomar medidas directamente en su proveedor de control de código fuente.

- Aborde las conclusiones: actualice su código según las directrices de corrección incluidas en las conclusiones y, a continuación, añada nuevas confirmaciones a la solicitud de cambios. AWS Security Agent analizará el código actualizado.
- Resolver conversaciones: después de abordar un problema de seguridad, marque la conversación como resuelta para hacer un seguimiento de su progreso.

> **Tip**
>
> Cada hallazgo incluye una guía de corrección específica adaptada al problema de seguridad identificado. Revise esta guía detenidamente para comprender el riesgo de seguridad y cómo abordarlo de manera eficaz.

Cómo filtrar los resultados de la revisión del código

Puede personalizar la forma en que AWS Security Agent analiza el código añadiendo un `filtering.md` archivo a su repositorio. Este archivo le permite reducir los falsos positivos al proporcionar un contexto sobre su base de código y excluir los archivos o carpetas del análisis.

Crear el archivo de filtrado

Cree un archivo con un nombre `filtering.md` en el `.awssecurityagent` directorio de la raíz de su repositorio:

```
.awssecurityagent/filtering.md
```

AWS Security Agent lee este archivo desde la rama principal de su repositorio (por ejemplo, `main` o`mainline`) al analizar las solicitudes de incorporación de cambios.

Estructura de archivos

El `filtering.md` archivo utiliza el formato Markdown estándar con secciones específicas que AWS Security Agent reconoce. El archivo debe incluir un `Code Review` encabezado seguido de una o ambas de las siguientes secciones: `IgnorePatterns` y `ContextHints` (sin espacios).

El siguiente ejemplo muestra la estructura completa de un `filtering.md` archivo:

```
# filtering.md

## Code Review

### IgnorePatterns

**/*.md

/myapp/src/**/*.snap

/myapp/config/README

### ContextHints

- The backend is a trusted system and won't return non-standard protocols.
- URL is generated from server with presigned token, so no SSRF security
 vulnerabilities.
- AppSec has verified that we are allowed to use cache with an eviction policy.
```

Ignora los patrones

`IgnorePatterns`En esta sección se especifican los archivos y las carpetas que AWS Security Agent debe omitir durante la revisión del código. Se utiliza `glob patterns` para definir qué rutas se van a excluir del análisis.

Requisitos de formato:

- Cada patrón debe estar en su propia línea.
- Separe cada patrón con una línea vacía entre ellos. Esto garantiza que el archivo se muestre correctamente cuando se visualice en nuestras GitHub herramientas de revisión de código.
- Los patrones siguen el formato global estándar. Por ejemplo, `**/*.md` hace coincidir todos los archivos de Markdown y `/myapp/src/**/*.snap` todos los `.snap` archivos de la `/myapp/src/` carpeta raíz.
- En esta sección, admitimos hasta 1000 patrones de ignorado.

Sugerencias de contexto

La `ContextHints` sección proporciona un contexto adicional sobre su base de código que ayuda a AWS Security Agent a realizar evaluaciones más precisas. Utilice sugerencias contextuales para explicar las decisiones arquitectónicas, las excepciones de seguridad u otra información que pueda afectar a la interpretación de los resultados.

Requisitos de formato:

- Cada sugerencia debe comenzar con un guión (`-`) seguido de un espacio.
- Escribe cada sugerencia como una sola línea de texto de formato libre limitado a 500 caracteres.
- Cada sugerencia debe describir un contexto específico sobre tu base de código.
- En esta sección, admitimos hasta 20 sugerencias de contexto.

Las sugerencias de contexto se aplican después de que AWS Security Agent complete su análisis inicial, lo que ayuda a filtrar los hallazgos que no se aplican a su caso de uso específico.

Siguientes pasos

Tras revisar los hallazgos de seguridad del código:

- Actualice el código según las directrices de corrección
- Impulsa nuevas confirmaciones para activar un nuevo análisis de tus cambios
- Ajuste la configuración de revisión de código si es necesario (consultethe section called “Habilitar la revisión del código de las solicitudes de extracción para los GitHub repositorios”)
- Revise los requisitos de seguridad de su organización para comprender los criterios de validación

- Considere la posibilidad de realizar pruebas de penetración para una validación exhaustiva de la seguridad de las aplicaciones implementadas

Crear una revisión de código

Cree revisiones de código en la aplicación web AWS Security Agent para analizar sus repositorios de código fuente y fuentes de S3 en busca de vulnerabilidades de seguridad. Las revisiones del código realizan un análisis estático exhaustivo de toda la base de código, identificando los problemas de seguridad y proporcionando orientación para solucionarlos.

A diferencia de la revisión del código basada en solicitudes de extracción, que analiza los cambios individuales en el código (consultethe section called “Revisa los hallazgos de seguridad del código en las solicitudes de cambios”), las revisiones de código bajo demanda escanean todo el código fuente para identificar las vulnerabilidades de seguridad y validar el cumplimiento de los requisitos de seguridad de la organización.

En este procedimiento, creará una revisión del código seleccionando las entradas del código fuente, configurando los permisos y realizando la revisión.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Acceso a la aplicación web AWS Security Agent
- Al menos un GitHub repositorio o depósito de S3 conectado en su espacio de agente

> **Tip**
>
> Si ya tiene GitHub repositorios conectados a su espacio de agente, la revisión del código está lista para su uso, sin necesidad de realizar ninguna configuración adicional. Selecciona Empezar en una aplicación web en la tarjeta de revisión del código de tu página de Agent Space o inicia la aplicación web directamente.
> Si necesita conectar fuentes adicionales o configurar buckets de S3, consultethe section called “Habilitar la revisión de código”.

Acceda a la página de reseñas de código

Navegue hasta la sección de revisiones de código en la aplicación web.

1. Inicie sesión en la aplicación web AWS Security Agent.
2. En la barra lateral izquierda, selecciona Reseñas de código.
3. Verás una lista de las revisiones de código existentes con la información de origen, el estado de la última ejecución y un resumen de los resultados.

Crea una revisión del código

Configure una nueva revisión de código configurando sus entradas y permisos de código fuente.

1. En la página de revisiones de código, selecciona Crear revisión de código.

Configure los detalles de la revisión del código

Proporcione un título y seleccione el código fuente que desee revisar.

1. En el campo Título, introduce un nombre descriptivo para la revisión del código.

> **Tip**
>
> Use un nombre que identifique la aplicación, el repositorio o el alcance de la revisión. Por ejemplo, «billing-service-security-review» o «infrastructure-code-audit».

2. En la sección Fuentes, selecciona las entradas de código fuente para esta revisión. Elija entre dos pestañas:

GitHub repositorios

Seleccione uno de los repositorios conectados a su espacio de agente.

1. Seleccione la pestaña de GitHub repositorios.
2. En la tabla de repositorios integrados, seleccione la casilla de verificación situada junto a cada repositorio que desee incluir en la revisión.
3. Usa el campo de búsqueda para buscar repositorios específicos por nombre.

> **Note**
>
> Aquí solo aparecen los repositorios conectados a su Agent Space mediante la configuración de revisión de código. Para añadir más repositorios, selecciona Administrar en la consola de administración o pídele al administrador que actualice la configuración del espacio de agente.

Orígenes de S3

Seleccione los archivos ZIP de los depósitos de S3 conectados a su espacio de agente. El administrador de Agent Space configura qué depósitos de S3 están disponibles. Cualquier archivo ZIP almacenado en uno de esos depósitos se puede utilizar como fuente para revisar el código.

1. Seleccione la pestaña de fuentes de S3.
2. Introduzca el URI de S3 de cada archivo ZIP que desee incluir en la reseña. Puede añadir hasta 30 fuentes S3.

> **Note**
>
> Las fuentes de S3 deben ser archivos ZIP almacenados en depósitos de S3 que estén conectados a su espacio de agente. Para que haya más depósitos disponibles, consulte. the section called “Habilitar la revisión de código”

Configuración de permisos

Seleccione la función de servicio de IAM y el grupo de CloudWatch registros opcional para esta revisión del código.

1. En la sección Permisos, busque el menú desplegable del rol de servicio.
2. Seleccione la función de IAM entre las funciones de servicio configuradas.

> **Note**
>
> El rol de servicio debe tener permisos para acceder al código fuente en S3 y escribir en CloudWatch los registros y en cualquier otro recurso de AWS necesario para la revisión

del código. Las funciones de servicio se configuran durante la configuración de la revisión del código en la consola de administración de AWS.

3. (Opcional) En el menú desplegable del grupo de CloudWatch registros, seleccione un grupo de registros para almacenar los registros de ejecución de las revisiones de código.

> **Note**
>
> Si no selecciona un grupo de registros, AWS Security Agent crea un grupo de registros predeterminado para almacenar los registros de revisión de código.

Configure la corrección automática del código

Habilite la corrección automática para que AWS Security Agent genere correcciones de código para todos los hallazgos tan pronto como se complete la revisión.

1. En la sección Corrección automática de códigos, seleccione la casilla Habilitar la corrección automática de códigos.

La forma en que AWS Security Agent ofrece la solución depende de la fuente:

- GitHub Repositorios privados: AWS Security Agent envía una solicitud de extracción con la corrección al repositorio.
- GitHub Repositorios públicos: para evitar revelar la vulnerabilidad antes de que se corrija, AWS Security Agent no abre una solicitud de extracción. En su lugar, añade una diferencia sugerida a la conclusión de que puede descargarla desde la aplicación web y solicitarla de forma privada.
- Fuentes S3: la corrección del código no está disponible. Revise los detalles de la búsqueda y aplique las correcciones manualmente.

> **Important**
>
> Todas las personas con acceso de lectura pueden ver las solicitudes de corrección enviadas a los repositorios privados. Revisa los cambios antes de unirlos. La corrección automática del código solo está disponible cuando se seleccionan GitHub los repositorios como fuente.

> **Note**
>
> Si está desactivada, puedes activar manualmente la corrección del código para cada GitHub-sourced hallazgo una vez finalizada la revisión.

Configure la validación simulada

Habilite la validación simulada para confirmar dinámicamente si las vulnerabilidades descubiertas se pueden explotar en una aplicación en ejecución.

1. En la sección Validación simulada, seleccione la casilla Habilitar la validación simulada.

Cuando está activado, AWS Security Agent aprovisiona un entorno simulado una vez finalizado el análisis estático. Incorpora el código fuente, inicia los servicios en el entorno e intenta aprovechar las vulnerabilidades detectadas durante el análisis. A continuación, los resultados se actualizan con un estado de validación que indica si la vulnerabilidad se ha aprovechado correctamente.

> **Note**
>
> En la actualidad, la validación simulada solo está disponible para aplicaciones dockerizables independientes. Cuando se seleccionan varios repositorios como fuentes, la validación simulada no está disponible.

> **Important**
>
> La validación simulada añade tiempo de procesamiento a la ejecución de revisión del código. El paso de validación proporciona un entorno y ejecuta intentos de explotación. Esto suele tardar de 1 a 3 horas, según el número de hallazgos y la complejidad de la aplicación.

Destinos de red permitidos

El entorno simulado tiene el acceso a la red saliente restringido a una lista de permitidos predefinida. La aplicación puede acceder a los siguientes dominios durante la validación:

En la siguiente tabla se enumeran los dominios permitidos y sus finalidades.

Dominio	Finalidad
`.amazonaws.com` , `.aws.amazon.com`	Servicios de AWS
`.public.ecr.aws`	Amazon ECR Public
`.docker.com` , `.docker.io`	Docker Hub
`.github.com` , `.githubusercontent.com`	GitHub
`.gitlab.com`	GitLab
`.npmjs.com` , `.npmjs.org`	registro npm
`.pypi.org` , `.pypi.python.org` , `.pythonhosted.org`	Índice de paquetes de Python
`.crates.io` , `.rustup.rs`	Paquetes de Rust
`.maven.org` , `.gradle.org`	Java/Gradle paquetes
`.nuget.org`	paquetes.NET
`.rubygems.org` , `.ruby-lang.org`	Paquetes de Ruby
`.golang.org` , `.pkg.go.dev` , `.goproxy.io`	Paquetes Go
`.nodejs.org` , `.yarnpkg.com`	Node.js

Dominio	Finalidad
`.alpinelinux.org` , `.debian.org` , `.ubuntu.com` , `.centos.org` , `.fedoraproject.org`	Repositorios de distribución de Linux
`.cloudfront.net`	CloudFront distribuciones
`.google.com` , `.googleapis.com`	API de Google
`.microsoft.com` , `.visualstudio.com`	Servicios de Microsoft
`.sourceforge.net` , `.bitbucket.org`	Alojamiento de origen

> **Note**
>
> Si su aplicación requiere acceso a la red a dominios que no figuran en esta lista, el firewall de la red bloqueará la conexión. Es posible que las aplicaciones que dependen de API o servicios externos que no figuran en la lista anterior no se inicien correctamente en el entorno simulado.

Cree la revisión del código

1. Revise la configuración para garantizar la precisión.
2. Seleccione Crear revisión de código.

Se le redirigirá a la página de detalles de la revisión del código, donde podrá iniciar una revisión.

Ejecuta una revisión del código

Tras crear una revisión del código, inicie una ejecución para iniciar el análisis.

1. En la página de detalles de la revisión del código, seleccione Iniciar revisión.

2. AWS Security Agent comienza a analizar el código fuente.

También puede iniciar una revisión desde la página de la lista de revisiones de código seleccionando Iniciar revisión junto a la revisión del código que desee ejecutar.

Supervisa una ejecución de revisión de código

Realice un seguimiento del progreso de la revisión del código a medida que se ejecuta.

Revisa las fases de ejecución

Una ejecución de revisión del código pasa por las siguientes fases, que se muestran como un indicador de progreso:

1. Preflight: AWS Security Agent valida el acceso al código fuente y configura el entorno de pruebas. Las comprobaciones previas a la verificación incluyen:
   - Configuración de la infraestructura de servicios
   - Validación del acceso a la fuente S3
   - Configuración del entorno de pruebas
2. Análisis estático: AWS Security Agent escanea el código fuente en busca de vulnerabilidades de seguridad e infracciones de requisitos.
3. Validación simulada (opcional): si la validación simulada está habilitada, AWS Security Agent aprovisiona un entorno simulado e implementa la aplicación. A continuación, intenta aprovechar las vulnerabilidades descubiertas durante el análisis estático. Este paso confirma si los hallazgos se pueden explotar en el tiempo de ejecución objetivo. Esta fase solo aparece cuando se habilita la validación simulada durante la creación de la revisión del código.
4. Finalización: AWS Security Agent recopila las conclusiones y genera el resumen de los resultados.

Vea los detalles de la ejecución

En la página de detalles de la ejecución, navega entre las pestañas para supervisar el progreso:

- Ejecución de revisión del código: consulta el resumen de la ejecución, que incluye el identificador de la ejecución, la hora de creación, el estado, la duración, las horas de la tarea, el desglose de los niveles de gravedad y el gráfico de tipos de riesgo.
- Verificación previa: consulta el progreso y el estado de la verificación previa de cada paso de validación.

- Registros de revisión de código: vea las tareas que el agente de seguridad de AWS identificó y llevó a cabo durante la revisión, con registros de tareas detallados para cada paso.
- Validación simulada: cuando la validación simulada esté habilitada, consulte el estado del aprovisionamiento, las tareas de validación para ver los hallazgos individuales y sus resultados.
- Hallazgos: consulte los hallazgos de seguridad una vez finalizada la revisión (consulte). the section called “Revise los resultados de una revisión del código”

Historial de ejecuciones

Cada revisión de código mantiene un historial de todas las ejecuciones. En la página de detalles de la revisión del código:

- La sección Última ejecución muestra la ejecución más reciente con su hora de inicio, estado, duración e ID.
- La tabla Todas las ejecuciones muestra todas las ejecuciones anteriores con su hora de inicio, estado, duración, resumen de los resultados e ID.
- Seleccione Supervisar la ejecución para ver los detalles de la última ejecución activa.
- Selecciona el enlace de la hora de inicio de cualquier ejecución para ver todos sus detalles.

Siguientes pasos

Tras realizar una revisión del código:

- Revise los hallazgos de seguridad y sus directrices de corrección (consultethe section called “Revise los resultados de una revisión del código”)
- Corrija los hallazgos mediante solicitudes de cambios automatizadas o correcciones manuales (consulte) the section called “Remediar los hallazgos de la revisión del código”
- Realice revisiones adicionales después de implementar las correcciones para verificar la corrección
- Ajusta la configuración o las fuentes de la revisión de código a medida que evoluciona tu base de código

Revise los resultados de una revisión del código

Una vez finalizada la revisión del código, revisa el resumen de la ejecución y las conclusiones de seguridad para comprender las vulnerabilidades del código fuente. Cada hallazgo contiene una descripción, un índice de gravedad, las ubicaciones de los códigos, un razonamiento de riesgo y sugerencias de correcciones para ayudarte a priorizar y abordar los problemas de seguridad.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Una revisión de código completada o en curso
- Acceso a la aplicación web AWS Security Agent

Paso 1: Acceda a la ejecución de revisión del código

Navegue hasta la revisión de código completa para ver el resumen y las conclusiones.

1. Inicie sesión en la aplicación web AWS Security Agent.
2. En la barra lateral izquierda, selecciona Reseñas de código.
3. Selecciona la revisión de código que deseas examinar.
4. En la tabla Todas las ejecuciones, seleccione la ejecución completada haciendo clic en su enlace de hora de inicio. Como alternativa, elija Supervisar la ejecución para ver la última ejecución.

Paso 2: Supervisa el progreso de la ejecución

Realice un seguimiento del progreso de su ejecución de revisión de código mediante el indicador de pasos.

1. Ubique el indicador de pasos horizontales debajo del encabezado de la página.
2. Revise el estado de cada fase:
   - Preflight: valida el acceso al código fuente y configura el entorno de escaneo. Las comprobaciones incluyen la configuración de la infraestructura de servicios, la validación del acceso a la fuente S3 y la configuración del entorno de pruebas, que incluye las comprobaciones de GitHub acceso.
   - Análisis estático: analiza el código fuente en busca de vulnerabilidades de seguridad e infracciones de los requisitos.

- Validación simulada (opcional): cuando está habilitada, proporciona un entorno simulado e intenta aprovechar las vulnerabilidades descubiertas contra la aplicación en ejecución.
- Finalización: compila las conclusiones y genera el resumen de los resultados.

> **Note**
>
> Cada paso muestra un indicador de estado (completado o en curso). La ejecución se habrá completado cuando todas las fases estén marcadas como Completadas. El paso de validación simulada solo aparece cuando se habilita la validación simulada durante la creación de la revisión del código.

Paso 3: Revisa el resumen de la ejecución

Navegue hasta la pestaña Ejecución de revisión de código para ver los resultados de alto nivel.

1. Seleccione la pestaña Ejecución de revisión de código.
2. La sección de resumen de la ejecución proporciona el estado, la duración y otros detalles de alto nivel de la ejecución. También proporciona un panel de control de los hallazgos de seguridad clasificados por nivel de gravedad y tipos de riesgo.
3. La descripción general de la aplicación realizada por AWS Security Agent proporciona un resumen del escaneo de revisión del código una vez finalizada la ejecución

Paso 4: Revise los resultados de la verificación previa

Vaya a la pestaña Preflight para comprobar que se han superado todas las comprobaciones de acceso a las fuentes.

1. Seleccione la pestaña Verificación previa.
2. Revise el indicador de progreso previo a la verificación que muestra el número de comprobaciones completadas.
3. Compruebe que cada comprobación muestre un estado de éxito:
   - Configuración de la infraestructura de servicios: confirma que el entorno de pruebas está listo
   - Validación del acceso a la fuente de S3: confirma el acceso al código fuente de S3 (si corresponde)

- Configuración del entorno de pruebas: confirma que el entorno de análisis está configurado

> **Note**
>
> Si se produce un error en alguna de las comprobaciones previas a la comprobación, la ejecución no procederá al análisis estático. Revise los detalles de la comprobación para identificar y resolver los problemas de acceso y, a continuación, inicie una nueva ejecución.

Paso 5: Revisa los registros de revisión del código

Vaya a la pestaña Registros de revisión de código para ver las tareas que AWS Security Agent realizó durante el análisis.

1. Seleccione la pestaña Registros de revisión de código.
2. Examine la lista de tareas en el panel izquierdo.
3. Seleccione una tarea para ver su registro detallado en el panel derecho.

> **Tip**
>
> Usa el campo de búsqueda para filtrar las tareas por nombre. Los registros proporcionan información sobre lo que examinó AWS Security Agent y cómo llegó a sus conclusiones.

Paso 6: Navegue hasta las conclusiones

Seleccione la pestaña Hallazgos para ver todos los hallazgos de seguridad de la ejecución.

> **Note**
>
> Filtro de confianza predeterminado
>
> De forma predeterminada, solo se muestran los resultados con un nivel de confianza alto por parte del agente. Para mostrar también los resultados con un nivel de confianza medio o bajo por parte de los agentes y los falsos positivos, desactive la opción Ocultar los hallazgos no verificados.

1. Seleccione la pestaña Hallazgos.
2. Los hallazgos se muestran en una vista dividida con la lista de hallazgos a la izquierda y los detalles del hallazgo seleccionado a la derecha.
3. Revisa la información que aparece en cada tarjeta de búsqueda:
   - Título de búsqueda: un nombre descriptivo que resuma el problema de seguridad
   - Insignia de gravedad: indicador de Color-coded gravedad:
     - Crítico (rojo): requiere una acción inmediata; la explotación podría comprometer el sistema
     - Alto (rojo): requiere atención inmediata; la explotación podría tener un impacto significativo en la seguridad
     - Medio (naranja): debe abordarse en un plazo razonable; contribuye al riesgo general de seguridad
     - Bajo (amarillo): se puede abordar como parte de un mantenimiento regular; el riesgo inmediato es mínimo
   - Última actualización: fecha y hora de la última actualización del hallazgo

Paso 7: Revise los detalles del hallazgo

Seleccione los hallazgos individuales para ver información completa sobre cada vulnerabilidad.

1. Seleccione un hallazgo en el panel izquierdo para mostrar sus detalles en el panel derecho.
2. Revisa las acciones disponibles:
   - Resolver el hallazgo: marca el hallazgo como resuelto después de abordarlo
   - Corregir el código: genera una solicitud de cambios con una solución (disponible para GitHub las fuentes)
3. Envía tus comentarios utilizando ¿Fue correcto este hallazgo? — Seleccione Sí o No para mejorar la precisión de los análisis futuros.
4. Revise los atributos clave en la sección de descripción general:
   - Confianza del agente: el nivel de confianza que tiene AWS Security Agent en este hallazgo
   - Gravedad: el nivel de riesgo con una insignia codificada por colores
   - Tipo de riesgo: la categoría de riesgo de seguridad
   - Estado de validación: cuando la validación simulada está habilitada, indica si se ha confirmado que el hallazgo es explotable en un entorno en ejecución:
     - Confirmado: la vulnerabilidad se aprovechó correctamente en el entorno simulado

- No se ha reproducido: no se pudo aprovechar la vulnerabilidad en el tiempo de ejecución de destino
- Validación fallida: el intento de validación no fue concluyente debido a un error
- No validado: no se realizó una validación simulada para este hallazgo. Esto ocurre cuando la validación no está habilitada o se ha agotado el tiempo de espera del paso de validación antes de llegar a esta conclusión.

- Resuelto: si el hallazgo se ha resuelto () Yes/No
- Última actualización: fecha y hora de la actualización más reciente

5. Amplíe la sección de descripción para que lea:
   - Una explicación detallada del problema de seguridad
   - ¿Cómo podría explotarse la vulnerabilidad
   - El posible impacto en su aplicación
   - Pasos de verificación que el agente realizó para confirmar el hallazgo
6. Amplíe la sección Ubicaciones de códigos para ver:
   - Rutas de archivo específicas en las que se identificó el problema
   - Una breve descripción de lo que se encontró en cada ubicación
   - Insignias de números de línea que enlazan con el código correspondiente
7. Amplíe la sección de pruebas para revisar:
   - El código, la configuración o las observaciones específicos que respaldan la conclusión
   - Una breve explicación de por qué cada elemento demuestra la vulnerabilidad
   - Los archivos afectados y los números de línea de cada prueba
8. Amplíe la sección Solución sugerida para ver:
   - Los cambios que AWS Security Agent recomienda para corregir el hallazgo
   - Ejemplo de código o configuración para cada cambio recomendado

> **Tip**
>
> Usa las ubicaciones de los códigos para navegar rápidamente a los archivos afectados en tu repositorio. Cada ubicación incluye el contexto suficiente para comprender el problema sin necesidad de leer todo el archivo.

Paso 8: Prioriza y aborda los hallazgos

Valide los hallazgos y tome medidas al respecto para corregir las vulnerabilidades y mejorar la seguridad de su aplicación.

Para detectar hallazgos de alta gravedad con un alto grado de confianza por parte de los agentes:

1. Revise detenidamente las secciones de descripción y ubicación del código.
2. Usa el código de remediación para generar una solicitud de cambios con una solución, o revisa las relaciones públicas de remediación automática si has activado esa opción.
3. Planifica una revisión del código de seguimiento para comprobar que la corrección es efectiva.

Para hallazgos de gravedad media con alta confianza por parte de los agentes:

1. Establezca prioridades en función de su tolerancia al riesgo y del contexto empresarial.
2. Incluya las tareas de remediación en su planificación habitual de los sprints de desarrollo.
3. Considere si varios hallazgos de gravedad media juntos crean un mayor riesgo.

Para los resultados de confianza media o baja:

1. Revise las secciones de descripción y ubicación del código para validar las suposiciones y las condiciones en las que se produce la vulnerabilidad.
2. Si la vulnerabilidad es válida, priorice en función de la gravedad y la tolerancia al riesgo y considere las tareas de corrección.

Paso 9: Realice un seguimiento del progreso de la remediación

Utilice la interfaz de resultados y vuelva a ejecutarlas para hacer un seguimiento de las vulnerabilidades que se han abordado.

1. A medida que vaya implementando las correcciones, utilice Resolve Finding para marcar las conclusiones como abordadas.
2. Realiza una nueva revisión del código para comprobar que las correcciones resuelven los hallazgos y no introducen nuevos problemas.
3. Revisa la tabla de todas las ejecuciones de la página de detalles de la revisión del código para comparar los resultados de las ejecuciones a lo largo del tiempo.

> **Tip**
>
> Tras combinar las solicitudes de cambios de corrección, inicia una nueva ejecución de la misma revisión de código para confirmar que las vulnerabilidades se han resuelto. Compara el recuento de resultados entre las ejecuciones para hacer un seguimiento de tu progreso.

Siguientes pasos

Tras revisar los resultados de la revisión del código:

- Priorice los hallazgos de alta gravedad con gran confianza para una remediación inmediata
- Utilice el código de Remediate para generar correcciones automatizadas de los GitHub-sourced hallazgos (consulte) the section called “Remediar los hallazgos de la revisión del código”
- Ejecute revisiones adicionales del código después de implementar las correcciones para verificar la corrección
- Ajuste las fuentes o la configuración de la revisión de código a medida que evolucione su base de código (consulte) the section called “Habilitar la revisión de código”

Remediar los hallazgos de la revisión del código

Tras revisar los hallazgos de seguridad de una revisión del código, puede usar AWS Security Agent para generar correcciones de código para los hallazgos en las fuentes GitHub del repositorio. En el caso de los repositorios privados, AWS Security Agent abre una solicitud de cambios con la solución propuesta. En el caso de los repositorios públicos, AWS Security Agent adjunta una diferencia descargable a la conclusión que puede aplicar localmente. Los hallazgos de las fuentes de S3 deben corregirse manualmente.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Una revisión completa del código realizada con los hallazgos
- GitHub repositorios conectados como fuente para la revisión del código
- Acceso a la aplicación web AWS Security Agent
- Familiaridad con la arquitectura y los requisitos de seguridad de su aplicación

Cómo funciona la corrección de código

Cuando se activa la corrección de código de un hallazgo, AWS Security Agent analiza el hallazgo y sus ubicaciones de código y, a continuación, genera una corrección de código. La forma en que se entrega la solución depende de la fuente:

- GitHub Repositorios privados: AWS Security Agent envía una solicitud de extracción al repositorio correspondiente. La solicitud de cambios incluye una descripción del problema de seguridad y de los cambios realizados.
- GitHub Repositorios públicos: AWS Security Agent adjunta una sugerencia de modificación al hallazgo para que la vulnerabilidad no se revele antes de corregirla. Puede descargar la diferencia desde la aplicación web y aplicarla localmente con ella. `git apply /path/to/code_remediation_changes.diff`
- Fuentes S3: la corrección del código no está disponible. Utilice la descripción del hallazgo, las ubicaciones del código y el razonamiento de riesgo para aplicar las correcciones manualmente.

> **Important**
>
> Las solicitudes de extracción creadas por AWS Security Agent están visibles para todos los usuarios que tienen acceso de lectura al repositorio. Revise los cambios antes de fusionarlos para asegurarse de que se ajusten a los requisitos de su aplicación.

Corrección automática del código

Si activó la corrección automática del código al crear la revisión del código, AWS Security Agent generará correcciones para todos los hallazgos válidos tan pronto como se complete la revisión. No necesita realizar ninguna acción adicional: las solicitudes de extracción aparecen en los GitHub repositorios privados conectados y las diferencias aparecen en los hallazgos de los GitHub repositorios públicos a medida que finaliza la ejecución.

Corrección manual del código

Si la corrección automática del código está deshabilitada, puede activar la corrección de los hallazgos individuales de las fuentes. GitHub

1. Diríjase a la pestaña Hallazgos de una ejecución de revisión de código completada.
2. Seleccione el hallazgo que desee corregir.

3. En el panel de detalles de búsqueda, elija Remediar código.
4. AWS Security Agent genera una corrección de código y envía una solicitud de extracción al repositorio o adjunta una diferencia descargable al hallazgo, en función de la visibilidad del repositorio.

Revise las solicitudes de extracción de correcciones

Después de que AWS Security Agent envíe una solicitud de extracción de correcciones a un repositorio privado GitHub :

1. Navegue hasta su repositorio. GitHub
2. Localice la solicitud de cambios creada por AWS Security Agent.
3. Revise los cambios, incluidos los siguientes:
   - La descripción en la que se explican el hallazgo y la solución de seguridad
   - Los cambios de código abordan la vulnerabilidad
   - Cualquier contexto relevante sobre el enfoque de remediación
4. Combina la solicitud de cambios si la solución es adecuada, o ciérrala e implementa una solución alternativa.

> **Tip**
>
> Tras fusionar las solicitudes de corrección, inicia una nueva revisión del código para comprobar que las correcciones resuelven los problemas detectados y no introducen nuevos problemas de seguridad.

Aplica las diferencias de corrección

Para los resultados de los GitHub repositorios públicos, aplique las diferencias descargables de forma local.

1. En el panel de detalles de búsqueda, descarga la diferencia de la sección de corrección del código.
2. En tu clon local del repositorio, ejecuta`git apply /path/to/code_remediation_changes.diff`.

3. Revisa los cambios aplicados, compruébalos con tu aplicación y aplícalos a través de tu flujo de trabajo de desarrollo normal.

Limitaciones

- La corrección del código solo está disponible para los hallazgos de las fuentes del GitHub repositorio. Los hallazgos de las fuentes de S3 se deben corregir manualmente.
- AWS Security Agent genera correcciones en función de su análisis de la vulnerabilidad. Revise todos los cambios antes de fusionarlos o confirmarlos para asegurarse de que son adecuados para su aplicación.
- Algunos hallazgos complejos pueden requerir una intervención manual que vaya más allá de la solución automática.

Siguientes pasos

Tras corregir los hallazgos:

- Revisa y fusiona las solicitudes de incorporación de datos en tus GitHub repositorios, o confirma las diferencias aplicadas a través de tu flujo de trabajo normal
- Realiza una nueva revisión del código para comprobar las correcciones y comprobar si hay problemas pendientes
- Resuelva los hallazgos en la aplicación web después de confirmar la corrección
- Ajuste las fuentes o la configuración de la revisión de código según sea necesario (consultethe section called “Habilitar la revisión de código”)

Ejecute un escaneo de código diferencial con S3

Ejecute un escaneo de código diferencial (diff) para analizar solo las líneas modificadas del código fuente, en lugar de realizar un escaneo completo del repositorio. Los escaneos diferenciales son más rápidos que los escaneos completos y producen resultados basados en cambios de código específicos, lo que los hace ideales para la validación previa a la fusión en los flujos de trabajo de desarrollo.

A diferencia de la revisión de código basada en solicitudes de extracción, que se activa automáticamente mediante eventos de proveedores de control de código fuente externos (consultethe section called “Revisa los hallazgos de seguridad del código en las solicitudes de

cambios"), los escaneos diferenciales se inician mediante programación a través de la API o el SDK de AWS Security Agent. Debe cargar un archivo diff unificado en S3 y hacer referencia a él al iniciar un trabajo de revisión de código.

Cómo funcionan los escaneos diferenciales

Un escaneo diferencial analiza los cambios de código en todo el contexto de su repositorio. Al crear un recurso de revisión de código con el código fuente cargado en S3, el escaneo diferencial utiliza todo el repositorio como contexto y, al mismo tiempo, centra los resultados específicamente en las líneas modificadas de la diferencia. Esto permite que el escaneo identifique los problemas de seguridad que se derivan de la forma en que los cambios interactúan con el código existente, como la interrupción de los flujos de autenticación, el manejo inseguro de los datos entre los módulos o los cambios que exponen las vulnerabilidades existentes.

El proceso de escaneo:. Debe cargar un archivo diff unificado (la salida de`git diff`) a un bucket de S3 conectado a su Agent Space. Llamas a la `StartCodeReviewJob` API con un `diffSource` parámetro que apunta a la ubicación en S3 de tu diferencial. AWS Security Agent analiza solo el código modificado en la diferencia para detectar vulnerabilidades de seguridad y cumplir con los requisitos de seguridad de su organización. Los resultados se basan en las líneas modificadas e incluyen índices de gravedad, ubicaciones de los códigos y directrices de corrección.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Un espacio de agentes con la revisión de código habilitada (consulte) the section called "Habilitar la revisión de código"
- Un recurso de revisión de código ya creado para el repositorio de destino, con todo el código fuente cargado en el depósito de S3 conectado a su espacio de agente. El repositorio completo proporciona un contexto que permite un análisis más profundo de la forma en que los cambios interactúan con el código existente. Consulta las the section called "Crear una revisión de código" instrucciones sobre cómo crear una revisión de código y cargar el código fuente.
- Un bucket de S3 conectado a su Agent Space
- Permisos de IAM para cargar archivos en el depósito de S3 y llamar `securityagent:StartCodeReviewJob`
- Un archivo de diferencias unificado generado a partir de los cambios en el código (por ejemplo, el resultado de`git diff main..feature-branch`)

> **Tip**
>
> Para obtener resultados más precisos, asegúrese de que su recurso de revisión de código tenga la última versión del código fuente completo cargada en S3. El análisis de diferencias utiliza este repositorio completo como contexto para comprender la arquitectura de la aplicación, los flujos de datos y los controles de seguridad existentes al analizar las líneas modificadas.

Paso 1: Genera un archivo diff

Genere una diferencia unificada que represente los cambios de código que desea escanear.

```
git diff main..feature-branch > changes.diff
```

Como alternativa, genere una diferencia para los cambios por etapas:

```
git diff --cached > changes.diff
```

> **Tip**
>
> El archivo diff debe estar en un formato diff unificado estándar. AWS Security Agent analiza las rutas de los archivos y cambia las líneas de los encabezados de las diferencias para abarcar su análisis.

Paso 2: Cargue la diferencia en S3

Cargue el archivo diff en un depósito de S3 que esté conectado a su espacio de agente.

```
aws s3 cp changes.diff s3://my-security-agent-bucket/diffs/changes.diff
```

> **Important**
>
> El depósito de S3 debe ser uno que ya esté conectado a su espacio de agente. El rol de servicio de IAM asociado a su espacio de agente debe tener acceso de lectura a esta

ubicación. Consulte las the section called “Habilitar la revisión de código” instrucciones sobre cómo conectar los buckets de S3.

Paso 3: Iniciar un trabajo de revisión del código diferencial

Llame a la `StartCodeReviewJob` API con el `diffSource` parámetro para iniciar un escaneo diferencial.

Mediante la AWS CLI

```
aws securityagent start-code-review-job \
  --agent-space-id "your-agent-space-id" \
  --code-review-id "your-code-review-id" \
  --diff-source '{"s3Uri": "s3://my-security-agent-bucket/diffs/changes.diff"}'
```

Uso del AWS SDK (Python)

```
import boto3

client = boto3.client('securityagent')

response = client.start_code_review_job(
    agentSpaceId='your-agent-space-id',
    codeReviewId='your-code-review-id',
    diffSource={
        's3Uri': 's3://my-security-agent-bucket/diffs/changes.diff'
    }
)

print(f"Job started: {response['codeReviewJobId']}")
```

Uso del AWS SDK (JavaScript/TypeScript)

```
import { SecurityAgentClient, StartCodeReviewJobCommand } from '@aws-sdk/client-
securityagent';

const client = new SecurityAgentClient({ region: 'us-east-1' });

const response = await client.send(new StartCodeReviewJobCommand({
```

```
  agentSpaceId: 'your-agent-space-id',
  codeReviewId: 'your-code-review-id',
  diffSource: {
    s3Uri: 's3://my-security-agent-bucket/diffs/changes.diff',
  },
}));

console.log(`Job started: ${response.codeReviewJobId}`);
```

La API se devuelve inmediatamente con un `codeReviewJobId` y `status` de`IN_PROGRESS`.

Paso 4: Supervise el escaneo

Compruebe el estado del trabajo de revisión del código hasta que se complete.

```
aws securityagent get-code-review-job \
  --agent-space-id "your-agent-space-id" \
  --code-review-id "your-code-review-id" \
  --code-review-job-id "the-job-id"
```

El trabajo pasa por las mismas fases que una revisión completa del código: comprobación previa → Análisis estático → Finalización. Los escaneos diferenciales suelen completarse más rápido que los escaneos completos porque analizan menos líneas de código.

Paso 5: revisión de resultados

Una vez finalizado el trabajo, enumere los resultados del trabajo de revisión de código.

```
aws securityagent list-findings \
  --agent-space-id "your-agent-space-id" \
  --code-review-id "your-code-review-id" \
  --code-review-job-id "the-job-id"
```

Cada resultado incluye:

- Una descripción del problema de seguridad
- El nivel de gravedad (crítico, alto, medio o bajo)
- Ubicaciones de código que hacen referencia a líneas específicas de la diferencia
- Razonamiento de riesgo que explica el impacto potencial
- Asesoramiento de corrección

Para obtener más información sobre cómo comprender los hallazgos y actuar en función de ellos, consultethe section called “Revise los resultados de una revisión del código”.

Cuotas y límites

- Número máximo de archivos modificados en una diferencia: 3000 archivos o 5 MB de tamaño total de la diferencia
- Los resultados se limitan a 30 por escaneo y se priorizan por gravedad (Crítico > Alto > Medio > Bajo)

Siguientes pasos

Tras realizar un escaneo diferencial:

- Revise los resultados y aplique las directrices de corrección (consultethe section called “Revise los resultados de una revisión del código”)
- Habilita los comentarios de las solicitudes de extracción para la revisión automática del código en cada solicitud de extracción (consultathe section called “Habilitar la revisión del código de las solicitudes de extracción para los GitHub repositorios”)
- Realice periódicamente una revisión completa del código para detectar problemas ajenos a los cambios individuales (consultethe section called “Crear una revisión de código”)
- Utilice la integración del IDE para ejecutar escaneos diferenciales directamente desde su entorno de desarrollo (consultethe section called “Ejecute escaneos de seguridad de código desde su IDE”)

Ejecute escaneos de seguridad de código desde su IDE

Ejecute escaneos de seguridad del código de AWS Security Agent directamente desde su IDE con Kiro o Claude Code. La integración con el IDE le permite escanear el código fuente local para detectar vulnerabilidades de seguridad, realizar escaneos diferenciales únicamente en el código modificado y revisar los modelos de amenazas de los documentos de diseño, todo ello sin salir del entorno de desarrollo. Los resultados aparecen junto con el código junto con una guía de corrección, y puede aplicar correcciones automatizadas directamente desde el IDE.

Cómo funciona la integración con el IDE

La integración del IDE utiliza el servidor MCP (Model Context Protocol) de AWS para conectar el IDE al servicio de AWS Security Agent:

1. El servidor MCP empaqueta el código fuente en un archivo ZIP.
2. El archivo se carga en un depósito de S3 que el servidor aprovisiona automáticamente en su cuenta de AWS.
3. El servidor llama a la API de AWS Security Agent para iniciar un análisis.
4. AWS Security Agent analiza el código para detectar las vulnerabilidades de seguridad y el cumplimiento de los requisitos de seguridad de su organización.
5. Los resultados se devuelven al IDE con las ubicaciones de los códigos, las descripciones, los índices de gravedad y las sugerencias de corrección.

El servidor MCP se encarga de toda la organización (aprovisionamiento del espacio de los agentes, creación de buckets de S3, configuración de roles de IAM, empaquetado de códigos y sondeos de escaneo), por lo que solo necesita las credenciales de AWS configuradas localmente.

> **Note**
>
> El único requisito previo son las credenciales de AWS configuradas en su entorno local (por ejemplo`aws configure`, mediante AWS SSO o variables de entorno). El servidor MCP aprovisiona automáticamente el espacio de agente, la función de servicio de IAM y el depósito de S3 la primera vez que se usa.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Credenciales de AWS configuradas localmente con los siguientes permisos:
  - `iam:CreateRole`, `iam:PutRolePolicy` (para configurar el rol de servicio una sola vez)
  - `s3:CreateBucket`, `s3:PutObject`, `s3:PutPublicAccessBlock`, `s3:PutLifecycleConfiguration`
  - `securityagent:CreateAgentSpace`, `securityagent:UpdateAgentSpace`, `securityagent:ListAgentSpaces`, `securityagent:BatchGetAgentSpaces`
  - `securityagent:CreateCodeReview`, `securityagent:StartCodeReviewJob`, `securityagent:BatchGetCodeReviewJobs`
  - `securityagent:ListFindings`, `securityagent:BatchGetFindings`
  - `securityagent:StartCodeRemediation`(para correcciones automatizadas)

  - `sts:GetCallerIdentity`
- uv installed (ejecutor de paquetes de Python)
- Python 3.10 o posterior
- Uno de los siguientes IDE:
  - Kiro (instale AWS Security Agent Power)
  - Claude Code (instale el complemento AWS Security Agent)

Instale el servidor MCP

Kiro

Instale AWS Security Agent Power desde el mercado de Kiro. The Power incluye la configuración del servidor MCP, las instrucciones de uso y los enlaces de ciclo de vida para ofrecer sugerencias de análisis de seguridad automáticos.

Como alternativa, configure el servidor MCP manualmente en su proyecto: `.kiro/mcp.json`

```
{
  "mcpServers": {
    "security-agent": {
      "command": "uvx",
      "args": ["awslabs.security-agent-mcp-server@latest"],
      "env": {
        "AWS_PROFILE": "default",
        "AWS_REGION": "us-east-1",
        "FASTMCP_LOG_LEVEL": "ERROR"
      }
    }
  }
}
```

Claude Code

Instale el complemento AWS Security Agent, que proporciona conocimientos para la configuración, los escaneos completos, los escaneos de diferencias, las revisiones de modelos de amenazas y la corrección.

Configure el servidor MCP en su proyecto: `.mcp.json`

```
{
  "mcpServers": {
    "awslabs.security-agent-mcp-server": {
      "command": "uvx",
      "args": ["awslabs.security-agent-mcp-server@latest"],
      "env": {
        "AWS_PROFILE": "default",
        "AWS_REGION": "us-east-1",
        "FASTMCP_LOG_LEVEL": "ERROR"
      }
    }
  }
}
```

> **Tip**
>
> También puede ejecutar el servidor MCP a través de Docker si prefiere no instalar Python localmente. Consulte la documentación del servidor MCP para ver la configuración de Docker.

First-time configuración

La primera vez que lo usa, el servidor MCP aprovisiona automáticamente los recursos de AWS necesarios:

Recurso	Convención de nombres	Finalidad
Agent Space	User-chosen o creado automáticamente	Contenedor para escaneos, revisiones y pruebas prelimina res
Rol de servicio de IAM	`SecurityAgentScanR ole`	Asumido por `securitya gent.amazonaws.com` para leer el código cargado
Bucket de S3	`security-agent-sca ns-{account}-{regi on}`	Almacena el código fuente comprimido (ciclo de vida de

Recurso	Convención de nombres	Finalidad
		caducidad automática de 30 días)

Para activar la configuración de forma explícita, pregunte a su IDE:

```
Set up the security agent
```

La configuración verifica sus credenciales de AWS, crea o reutiliza un espacio de agente, aprovisiona la función de IAM y el segmento de S3, y confirma la disponibilidad. Si ya dispone de Agent Spaces en la consola de administración de AWS, la configuración los muestra y le pregunta cuál debe usar.

> **Note**
>
> La configuración se ejecuta automáticamente en el primer escaneo si aún no está configurada. No es necesario ejecutarlo por separado.

Ejecute un análisis de seguridad completo

Analice todo su proyecto en busca de vulnerabilidades de seguridad:

```
Scan this project for security issues
```

El IDE:

1. Archiva tu código fuente (excluyendo `.gitnode_modules`, crea artefactos y otros directorios no esenciales)
2. Carga el archivo en S3
3. Inicia un trabajo completo de revisión de código
4. Las encuestas deben completarse (normalmente alrededor de 1 hora)
5. Presenta los hallazgos agrupados por gravedad

Progreso del escaneo

Los escaneos completos suelen tardar alrededor de 1 hora, según el tamaño de la base de código. El IDE comprueba el progreso cada 5 minutos y le notifica cuando los resultados están listos. Puede solicitar el estado en cualquier momento:

```
How's the scan going?
```

Ejecute un escaneo diferencial

Para obtener comentarios más rápidos durante el desarrollo, escanea solo el código que ha cambiado desde una referencia de git:

```
Scan my changes against main for security issues
```

De forma predeterminada, si no especificas una referencia base, el escaneo compara los cambios no confirmados con los cambios no confirmados. `HEAD` Puedes especificar de forma explícita una base diferente:

```
Diff scan my uncommitted changes
```

Los escaneos diferenciales cargan tanto el contexto completo del repositorio como el parche de git diff y, a continuación, ejecutan un análisis centrado únicamente en las líneas modificadas. Los resultados suelen llegar en un plazo de 5 a 15 minutos.

Para obtener más información sobre la API de escaneo de diferencias de S3, consulte. the section called “Ejecute un escaneo de código diferencial con S3”

Realice una revisión del modelo de amenazas

Analice los documentos de diseño para detectar cambios en la postura de seguridad mediante la metodología STRIDE:

```
Run a threat model review on my spec
```

El IDE identifica tus `requirements.md` `design.md` archivos (normalmente por debajo `.kiro/specs/`), los carga junto con el código fuente y realiza un análisis del modelo de amenazas. Los resultados identifican:

- Amenazas a la seguridad clasificadas por STRIDE (suplantación de identidad, manipulación, repudio, divulgación de información, denegación de servicio, aumento de privilegios)
- Clasificaciones de gravedad de cada amenaza
- Impacto en activos específicos de su base de código
- Recomendaciones de mitigación

> **Tip**
>
> Realice una revisión del modelo de amenazas antes de generar tareas de implementación a partir de una especificación. Esto detecta los problemas de diseño de seguridad antes de escribir el código.

Revisión de resultados

Cuando se completa un escaneo, los resultados aparecen en el IDE agrupados por gravedad:

```
# CRITICAL: SQL Injection in user-service.ts
   File: src/api/user-service.ts:45
   User input flows directly into SQL query without parameterization

# HIGH: Hardcoded credentials in config.ts
   File: src/config/database.ts:12
   Database password stored in source code
```

También se redacta un informe detallado `.security-agent/findings-{scan_id}.md` con información completa de cada hallazgo, incluidos el tipo de riesgo, la puntuación de confianza, la ubicación de los códigos y el código de corrección.

Para ver los resultados de una exploración anterior:

```
Show my security findings
```

Aplique correcciones automatizadas

Tras revisar los resultados, aplique una corrección automática:

```
Fix the security findings
```

El IDE analiza los hallazgos de arriba abajo por gravedad (Crítico → Alto → Medio → Bajo) y aplica las correcciones de código siguiendo las instrucciones de corrección de cada hallazgo. Una vez aplicadas todas las correcciones, ejecuta automáticamente un análisis de las diferencias de verificación para confirmar que los problemas se han resuelto.

También puedes corregir los resultados individuales:

```
Fix the SQL injection in user-service.ts
```

> **Important**
>
> Revisa siempre las correcciones automatizadas antes de comprometerlas. Compruebe que las correcciones no rompan la funcionalidad existente ni introduzcan regresiones.

Sugerencias de escaneo automático (Kiro)

Al usar Kiro Power, AWS Security Agent puede sugerir automáticamente escaneos de diferencias después de realizar cambios de código sensibles a la seguridad. The Power instala un gancho que evalúa cada turno de codificación completado y sugiere escanearlo cuando se produzcan cambios:

- Lógica de autenticación o autorización
- Criptografía o manejo de secretos
- Validación de entradas o saneamiento de datos
- Solicitudes de red o integraciones externas
- Configuración de seguridad (CORS, encabezados, gestión de sesiones)

Puede optar por no recibir sugerencias automáticas en cualquier momento eliminándolas. `.kiro/hooks/security-diff-scan-suggester.kiro.hook`

Tipos de escaneo disponibles

Tipo de análisis	Duración	Caso de uso	Comando
Análisis completo	Alrededor de 1 hora	Revisión exhaustiv a de toda la base de código	«Escanea mi proyecto para detectar

Tipo de análisis	Duración	Caso de uso	Comando
			problemas de seguridad»
Escaneo de diferencias	De 5 a 15 minutos	Solo se modificó el código (previo a la confirmación, previo a las relaciones públicas)	«Escanear mis cambios» o «Escanear diferencias con el archivo principal»
Modelo de amenaza	De 5 a 30 minutos	Documentos de diseño (requirements.md, design.md)	«Realice una revisión del modelo de amenazas según mis especificaciones»

Variables de entorno

Variable	Description (Descripción)	Predeterminado
`AWS_REGION`	Región de AWS para llamadas a SecurityAgent la API	`us-east-1`
`AWS_PROFILE`	Nombre del perfil de credenciales de AWS	Perfil predeterminado
`FASTMCP_LOG_LEVEL`	Nivel de registro del servidor MCP (DEPURACIÓN, INFORMACIÓN, ADVERTENCIA, ERROR)	`WARNING`

Resolución de problemas

«No está configurado. Ejecute primero la configuración».

`.security-agent/config.json`Falta el tuyo o el espacio de agentes ya no existe. Pide al IDE que ejecute la configuración:

```
Set up the security agent
```

El escaneo falla con AccessDenied

Asegúrese de que sus credenciales de AWS tengan los permisos de IAM necesarios que se indican en la sección Requisitos previos. El permiso que falta con más frecuencia es `iam:CreateRole` (necesario solo para la configuración inicial).

El escaneo se agota o tarda demasiado

- Los escaneos completos en bases de código grandes pueden tardar más de 1 hora
- Utilice escaneos diferenciales para el desarrollo iterativo: se completan en minutos
- Compruebe que su archivo fuente no incluya directorios innecesarios (el servidor MCP excluye automáticamente los patrones comunes)

Diferencia vacía: no hay cambios que escanear

Si realiza un análisis de diferencias sin cambios pendientes, el servidor MCP muestra el mensaje «Sin cambios frente a HEAD» y no inicia el análisis. Primero confirme o organice los cambios, o especifique una referencia base diferente.

Cuotas y límites

- Tamaño máximo del archivo fuente: 2 GB
- Ciclo de vida del bucket de S3: el código cargado se elimina automáticamente después de 30 días

Siguientes pasos

Tras ejecutar el primer análisis de seguridad del IDE:

- Habilite los comentarios de revisión del código de las solicitudes de extracción para una GitHub integración automática (consultethe section called “Habilitar la revisión del código de las solicitudes de extracción para los GitHub repositorios”)
- Configure los requisitos de seguridad para la validación de políticas específicas de la organización (consulte) the section called “Gestione los requisitos de seguridad”
- Realice escaneos completos periódicos para detectar problemas en toda su base de código (consulte) the section called “Crear una revisión de código”

- Utilice las revisiones de los modelos de amenazas sobre las nuevas especificaciones de las funciones antes de implementarlas

Crea una prueba de penetración

Configure las pruebas de penetración automatizadas para sus aplicaciones web configurando el alcance de la prueba, los dominios de destino y el acceso a los recursos de AWS. Las pruebas de penetración ayudan a identificar las vulnerabilidades de seguridad en las aplicaciones en ejecución mediante la simulación de escenarios de ataque reales contra sus dominios verificados.

AWS Security Agent realiza pruebas de seguridad exhaustivas en sus aplicaciones web en función del alcance y los permisos configurados, lo que proporciona información detallada sobre las vulnerabilidades explotables antes de que los atacantes puedan descubrirlas.

En este procedimiento, creará una prueba de penetración configurando los detalles de la prueba, definiendo el alcance de la prueba y configurando los permisos necesarios.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Acceso a la aplicación web AWS Security Agent
- Al menos un dominio verificado para realizar pruebas
- Función de IAM con los permisos adecuados para AWS Security Agent
- Comprensión de la arquitectura y las rutas críticas de su aplicación

Comience a crear una prueba de penetración

Navegue hasta la página de creación de la prueba de penetración en la aplicación web Agent.

1. Inicie sesión en la aplicación web AWS Security Agent.
2. Diríjase a la sección Pruebas de penetración.
3. Selecciona Crear una prueba de penetración.

> **Tip**
>
> Solo los dominios verificados se pueden incluir en las pruebas de penetración. Pida a su administrador que verifique el dominio en la consola de administración de AWS. Consulte the section called “Habilitar un dominio de aplicación para las pruebas de penetración”.

Asigne un nombre a su prueba de penetración

Proporcione un nombre descriptivo que ayude a identificar el propósito y el alcance de esta prueba de penetración.

1. En el campo Nombre de la prueba de penetración, introduzca un nombre descriptivo para la prueba de penetración.

   Example

   El nombre debe identificar claramente la aplicación, el entorno o el componente que se está probando. 100 caracteres como máximo.

Configure el alcance de la prueba de penetración

Defina qué dominios y rutas URL se probarán y configure las exclusiones opcionales para controlar los límites de las pruebas.

Agregue los dominios de destino

Especifique los dominios verificados que se probarán activamente para detectar vulnerabilidades de seguridad.

1. En la sección Alcance de la prueba de penetración, localice las URL de destino.
2. Amplía la sección Dominios verificados para ver los dominios disponibles.
3. En el campo URL de destino, introduce la URL de un dominio de destino.

> **Important**
>
> Solo se pueden probar los dominios verificados. La URL debe estar en un dominio que haya verificado previamente en AWS Security Agent. Sub-domains de un dominio verificado no requieren una verificación independiente.

4. Para añadir varios dominios de destino:
   a. Elija Añadir dominio.
   b. Introduzca la URL de cada dominio adicional.
5. Para eliminar un dominio de destino, selecciona Eliminar junto a la URL del dominio.

> **Tip**
>
> Para obtener los mejores resultados, incluye todos los dominios que forman parte del flujo de usuarios de tu aplicación, incluidos los subdominios para las API, los servicios de autenticación y la entrega de contenido. Sub-domains de un dominio principal verificado no requieren una verificación independiente.

Excluir los tipos de riesgo (opcional)

Elija categorías de riesgo específicas para excluirlas de las pruebas si no son aplicables a su aplicación.

1. Localice el campo Excluir tipos de riesgo.
2. Seleccione el menú desplegable para ver los tipos de riesgo disponibles.
3. Seleccione uno o más tipos de riesgo para excluirlos de la prueba de penetración.

> **Note**
>
> La exclusión de los tipos de riesgo limita el alcance de las pruebas. Excluya únicamente los tipos de riesgo que no sean relevantes para su aplicación o que desee probar por separado.

Agregue rutas URL fuera del ámbito de aplicación (opcional)

Especifique las rutas URL que no se deben probar durante la prueba de penetración. AWS Security Agent excluye la ruta especificada y todas las rutas anidadas debajo de ella. Por ejemplo, si la agrega `https://example.com/admin` como una URL fuera del alcance, `https://example.com/admin/tools` también estará fuera del alcance.

1. Busca la sección de Out-of-scope direcciones URL.
2. En el campo de entrada de Out-of-scope direcciones URL, introduce una ruta URL para excluirla (por ejemplo, `/admin/delete` o`/api/reset`).

> **Warning**
>
> Out-of-scope las rutas no se prueban para detectar vulnerabilidades. Asegúrese de excluir solo las rutas a las que no se debe acceder durante las pruebas, como las operaciones destructivas o las funciones administrativas confidenciales.

3. Para añadir varias rutas fuera del alcance:
   a. Selecciona Añadir URL.
   b. Introduzca cada ruta adicional.
4. Para eliminar una ruta, seleccione Eliminar junto a la ruta.

Agrega dominios accesibles (opcional)

Especifique los dominios que son necesarios para la prueba pero que no son objetivos de las pruebas de vulnerabilidad.

1. Busque la sección URL accesibles.
2. En el campo de entrada URL accesibles, introduce un dominio al que se pueda acceder durante las pruebas.

> **Note**
>
> Añade dominios accesibles para servicios de terceros (como Okta, Auth0 o Stripe) que estén fuera de tu dominio de destino. Esto es necesario para que AWS Security Agent pueda acceder a estas URL para iniciar sesión y navegar durante las pruebas. AWS Security Agent NO realiza pruebas de penetración en estos dominios, sino que se utilizan

únicamente con fines de acceso. Los dominios accesibles no requieren la verificación de propiedad, incluso si pertenecen a un dominio diferente al de destino. Solo los dominios de destino requieren una propiedad verificada.

3. Para añadir varios dominios accesibles:
   a. Selecciona Añadir URL.
   b. Introduce cada dominio adicional.
4. Para eliminar un dominio, selecciona Eliminar junto al dominio.

Agrega encabezados HTTP personalizados (opcional)

Especifique los encabezados HTTP personalizados que se añadirán a cualquier solicitud que realice AWS Security Agent durante las pruebas de penetración.

1. Busque la sección de encabezados HTTP personalizados.
2. En el campo de entrada de encabezados HTTP personalizados, ingresa el nombre y el valor del encabezado que se asociarán a las solicitudes salientes.

> **Note**
>
> De forma predeterminada, AWS Security Agent añade un encabezado personalizado para User-Agentestablecer en securityagent, a menos que se especifique un valor de User-Agentencabezado personalizado diferente.

3. Para añadir varios encabezados personalizados:
   a. Elija Agregar encabezado.
   b. Introduce cada encabezado personalizado adicional.
4. Para eliminar un encabezado personalizado, selecciona Eliminar junto al encabezado.

Configure el rol de IAM

Seleccione el rol de servicio preconfigurado para esta prueba de penetración. AWS Security Agent utiliza un modelo de Space-based permisos de agente en el que los administradores configuran las funciones de IAM al configurar su espacio de agente. Puede seleccionar entre las funciones que ya están configuradas y listas para usarse.

1. En la sección Permisos, busca el menú desplegable de roles de servicio.
2. Seleccione la función de IAM que concede a AWS Security Agent acceso a los recursos de AWS necesarios.

> **Important**
>
> El rol de IAM seleccionado debe tener permisos para acceder a los recursos de la VPC CloudWatch , los registros y cualquier otro servicio de AWS necesario para la prueba de penetración. Compruebe que el rol tenga la relación de confianza correcta con AWS Security Agent.

3. Localice el menú desplegable del grupo de CloudWatch registros.
4. Seleccione el grupo de registros en el que se almacenarán los registros de las pruebas de penetración. (opcional)

> **Note**
>
> El grupo de CloudWatch registros seleccionado almacenará registros detallados de la ejecución de la prueba de penetración, incluidas las solicitudes realizadas, las respuestas recibidas y las vulnerabilidades descubiertas.
> Si no selecciona un grupo de registros, se creará automáticamente un nuevo grupo de CloudWatch registros con el `/aws/securityagent` prefijo para almacenar los registros de las pruebas de penetración.

Corrección automática del código

Seleccione la casilla de verificación Habilitar la corrección automática.

> **Important**
>
> Para corregir los problemas de seguridad en sus repositorios de código fuente, AWS Security Agent puede enviar solicitudes de extracción a sus repositorios. Las solicitudes de extracción pueden estar visibles para todos los usuarios que tengan acceso de lectura a los repositorios.

Configurar los recursos de VPC (opcional)

Si sus dominios de destino son privados y están alojados en una VPC, configure los ajustes de la VPC en los que AWS Security Agent debe ejecutar las pruebas de penetración. Este paso solo es necesario para las aplicaciones que no son de acceso público.

> **Note**
>
> Omita este paso si sus dominios de destino son de acceso público. La configuración de VPC solo es necesaria para probar aplicaciones privadas alojadas en Amazon Virtual Private Cloud.

Elija la VPC, las subredes y los grupos de seguridad para el entorno de pruebas de penetración.

1. En la sección VPC, localice el menú desplegable de ID de VPC.
2. Seleccione la VPC en la que están alojados los dominios de destino.

> **Important**
>
> La VPC seleccionada debe contener los dominios de destino que especificó en el paso 3. Asegúrese de que la VPC tenga la configuración de red y enrutamiento adecuada para permitir que AWS Security Agent acceda a sus aplicaciones.

3. Localice el menú desplegable de subredes.
4. Seleccione una o más subredes en las que deba ejecutarse la prueba de penetración.

> **Note**
>
> Elija subredes que tengan acceso de red a las aplicaciones de destino. La prueba de penetración se ejecutará a partir de los recursos desplegados en estas subredes.

5. Localice el menú desplegable del grupo de seguridad.
6. Seleccione el grupo de seguridad que controla el acceso a la red para la prueba de penetración.

> **Important**
>
> El grupo de seguridad seleccionado debe permitir el tráfico saliente a sus dominios de destino y a cualquier dominio accesible. Asegúrese de que las reglas del grupo de seguridad permitan el acceso a la red necesario para realizar pruebas exhaustivas.

Configure las credenciales de autenticación (opcional)

Si sus dominios de destino requieren autenticación, proporcione credenciales para permitir que AWS Security Agent acceda a las áreas protegidas de su aplicación durante las pruebas de penetración. Este paso solo es necesario para las aplicaciones que requieren la autenticación del usuario.

> **Note**
>
> Omita este paso si sus dominios de destino no requieren autenticación o si todas las áreas que desea probar son de acceso público. Configure las credenciales solo cuando necesite que AWS Security Agent pruebe las secciones autenticadas de su aplicación.

Agregación de credenciales de

Proporcione las credenciales de autenticación que AWS Security Agent utilizará para acceder a su aplicación.

1. En la sección Credencial #1, seleccione un método de entrada de credenciales:
   - Introduzca las credenciales: introduzca las credenciales directamente en AWS Security Agent.
   - Configuración avanzada: para obtener información confidencial sobre credenciales, utilice opciones avanzadas, como las funciones de AWS Secrets Manager o AWS Lambda. Para obtener más información, consulte the section called “Proporcione credenciales de autenticación para las pruebas de penetración”.

     > **Tip**
     >
     > Para entornos de producción o credenciales confidenciales, recomendamos utilizar la opción de configuración avanzada para hacer referencia de forma segura a las

credenciales almacenadas en AWS Secrets Manager o Systems Manager Parameter Store.

Introduzca los detalles de las credenciales

Proporcione el nombre de usuario y la contraseña de la cuenta autenticada.

1. En el campo Nombre de usuario, introduzca el nombre de usuario para la autenticación.
2. En el campo Contraseña, introduzca la contraseña para la autenticación.

> **Important**
>
> Asegúrese de que las credenciales que proporcione tengan los niveles de acceso adecuados para las áreas que desee probar. Las credenciales deben representar el nivel de acceso de un usuario típico y no los privilegios administrativos.

Seleccione el dominio de acceso

Especifique qué dominio de destino utilizará estas credenciales para la autenticación.

1. En el menú desplegable Dominio de acceso, selecciona el dominio en el que se usarán estas credenciales.

> **Note**
>
> Si tiene varios dominios de destino que requieren credenciales diferentes, puede agregar conjuntos de credenciales adicionales haciendo clic en Agregar otra credencial después de completar esta configuración de credenciales.

Configure el mensaje de inicio de sesión del agente (opcional)

Proporcione instrucciones para guiar a AWS Security Agent a través del proceso de autenticación de su aplicación.

1. Amplíe la sección de solicitudes de inicio de sesión del agente si su flujo de autenticación requiere instrucciones específicas.

2. Introduzca instrucciones que describan cómo utilizar las credenciales proporcionadas en el flujo de inicio de sesión de su aplicación.

> **Note**
>
> El mensaje de inicio de sesión del agente le indica al agente cómo aplicar sus credenciales a su aplicación. Esto resulta útil para flujos de autenticación complejos, procesos de inicio de sesión de varios pasos o aplicaciones con procedimientos de inicio de sesión no estándar. Incluye instrucciones paso a paso, como «Navega hasta /login, introduce el nombre de usuario en el campo «Correo electrónico», introduce la contraseña y selecciona «Iniciar sesión».

Agrega varias credenciales (opcional)

Si su aplicación requiere varios conjuntos de credenciales o si los distintos dominios necesitan una autenticación independiente, añada conjuntos de credenciales adicionales.

1. Tras completar la primera configuración de credenciales, elija Añadir otra credencial.
2. Repita los pasos de configuración de credenciales para cada conjunto de credenciales adicional.
3. Para eliminar un conjunto de credenciales, seleccione Eliminar junto al encabezado de credenciales.

> **Tip**
>
> Configure varias credenciales al probar diferentes roles de usuario, acceder a varios dominios autenticados o verificar los controles de acceso basados en roles en su aplicación.

Adjunta recursos adicionales (opcional)

Proporcione recursos adicionales para ayudar a AWS Security Agent a realizar pruebas de penetración más exhaustivas y precisas. Los recursos adicionales pueden incluir diagramas de arquitectura, documentación de la API, archivos de configuración, GitHub repositorios o S3-hosted materiales que proporcionan un contexto sobre su aplicación.

> **Note**
>
> Los recursos adicionales son opcionales, pero se recomiendan. Proporcionar información completa sobre su aplicación ayuda a garantizar una cobertura exhaustiva de las pruebas, reduce los falsos positivos y ofrece resultados más procesables.

Añada recursos a la prueba de penetración

Seleccione los recursos existentes o cargue nuevos archivos que sirvan de guía para la prueba de penetración.

1. En la sección Recursos conectados, puedes:
   - Elija Seleccionar entre los disponibles para elegir entre los recursos que ya están conectados a AWS Security Agent (como GitHub repositorios o buckets de S3).
   - Elija Cargar para añadir nuevos archivos directamente desde su sistema local.

> **Tip**
>
> Entre los recursos útiles se incluyen la documentación de la API, los diagramas de arquitectura, OpenAPI/Swagger las especificaciones, los archivos de configuración, los diagramas de flujo de autenticación y cualquier otro material que describa la estructura y el comportamiento de la aplicación.

Seleccione uno de los recursos disponibles

Elija entre los recursos que ya están integrados con AWS Security Agent.

1. Elija Seleccione entre los recursos existentes.
2. Examine la lista de recursos disponibles de las fuentes conectadas, como:
   - GitHub repositorios, en la pestaña GitHub repositorios
   - Buckets de S3
   - Archivos subidos anteriormente
   - Repositorios de documentación
3. Seleccione los recursos que desee incluir en la prueba de penetración.

4. Seleccione Añadir a la prueba de penetración para adjuntar los recursos seleccionados.

Example

Te recomendamos seleccionar y añadir GitHub los repositorios pertinentes a tu pentest, de modo que AWS Security Agent pueda comprender el contexto de tu aplicación y generar correcciones de código listas para su implementación mediante solicitudes de cambios (cuando estén habilitadas)

> **Note**
>
> Los recursos seleccionados de las fuentes disponibles permanecen sincronizados con su ubicación original. Si actualiza un GitHub repositorio o un archivo S3, la prueba de penetración utilizará la versión actualizada.

> **Note**
>
> Si tiene una VPC privada asociada a su pentest y un GitHub repositorio configurado, asegúrese de que GitHub se pueda acceder a ella a través de su VPC privada para extraer recursos. GitHub En la mayoría de los casos, tendrá que asegurarse de que el tráfico saliente a través de la puerta de enlace NAT de VPC esté permitido de forma predeterminada o configurar reglas específicas para permitir el tráfico saliente GitHub para las IP (GitHub consulte Meta API Endpoint)

Cargue nuevos recursos

Cargue los archivos directamente desde su sistema local o proporcione contenido de texto sin formato a AWS Security Agent.

1. Seleccione Cargar.
2. Elija uno de los siguientes métodos de entrada:
   - Cargar archivos locales: seleccione uno o más archivos de su sistema local.
   - Pegar texto sin formato: escriba o pegue el contenido del texto directamente en el campo de entrada. Seleccione Cargar.
3. A continuación, selecciona Añadir para completar la carga.
4. Los recursos cargados aparecen en la tabla Recursos conectados.

> **Tip**
>
> Utilice la opción de texto sin formato cuando desee proporcionar rápidamente listas de puntos de conexión de las API, patrones de URL, instrucciones de prueba u otra información basada en texto sin necesidad de crear un archivo independiente.

> **Important**
>
> Asegúrese de que los archivos cargados y el contenido pegado no contengan información confidencial, como credenciales de producción, claves privadas o información de identificación personal (PII). Utilice versiones depuradas de los archivos y la documentación de configuración.

Conecta los recursos existentes

Los recursos existentes pueden provenir de lo que cargó anteriormente en AWS Security Agent, de su bucket de S3 y de sus GitHub repositorios integrados. Elija Seleccionar entre los recursos existentes para seleccionarlos.

Administre los recursos conectados

Revise, organice y elimine los recursos adjuntos a la prueba de penetración.

La tabla de recursos conectados muestra todos los recursos incluidos en la prueba de penetración con la siguiente información:

- Nombre: el nombre del archivo o el identificador del recurso
- Tipo: la categoría de recursos (archivos subidos, recursos de S3, GitHub repositorios, etc.)

Para gestionar los recursos:

1. Seleccione uno o más recursos mediante las casillas de verificación.
2. Selecciona Eliminar de la prueba de penetración para separar los recursos seleccionados.

> **Note**
>
> Puede ordenar la tabla por nombre o tipo haciendo clic en los encabezados de las columnas. Esto ayuda a organizar los recursos al trabajar con muchos archivos.

Cree la prueba de penetración

Finalice e inicie la configuración de la prueba de penetración.

Tras configurar todos los ajustes, estará listo para crear la prueba de penetración.

1. Revise todas las secciones de configuración para garantizar la precisión.
2. Elija una de las siguientes opciones:
   - Seleccione Crear penetración para guardar la configuración sin ejecutarla inmediatamente.
   - Seleccione Crear y ejecutar para guardar la configuración e iniciar inmediatamente la prueba de penetración.
   - Seleccione Cancelar para descartar la configuración de la prueba de penetración.

> **Important**
>
> Antes de ejecutar una prueba de penetración, compruebe que:
>
> - Todos los dominios de destino están correctamente verificados y son accesibles
> - Los roles de IAM tienen los permisos adecuados
> - Out-of-scope las rutas están configuradas correctamente para evitar que se prueben operaciones destructivas
> - Tiene autorización para realizar pruebas de seguridad en todos los dominios de destino

> **Note**
>
> Una vez que comience la prueba de penetración, puede supervisar su progreso desde la sección Ejecuciones de pruebas de penetración. La prueba puede tardar varias horas en completarse. La mayoría se completa en 16 horas, según el alcance y la complejidad de la aplicación.

Revise los resultados de una prueba de penetración

Supervise la ejecución de las pruebas de penetración en tiempo real en la página de registros de las pruebas de penetración después de que AWS Security Agent inicie una prueba de penetración. El agente de seguridad de AWS registra todas las acciones durante la prueba de penteo. Una vez finalizada, revise el resumen de la prueba preliminar, que incluye una descripción general de la aplicación, la cobertura con los puntos de enlace identificados y la evaluación de riesgos de los hallazgos de seguridad.

Evalúe los hallazgos de seguridad para abordar las vulnerabilidades de las aplicaciones. Cada hallazgo contiene la evaluación del impacto, el índice de gravedad, las pruebas justificativas y los detalles de las solicitudes de corrección (cuando la corrección automática del código está habilitada).

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Una prueba de penetración completada o en curso
- Acceso a la aplicación web AWS Security Agent

Paso 1: Acceda a la ejecución de la prueba de penetración

Navegue hasta la prueba de penetración realizada para ver las páginas de información general, registros y resultados.

1. Inicie sesión en la aplicación web AWS Security Agent.
2. Diríjase a la sección Pruebas de penetración.
3. Seleccione de la lista la prueba de penetración que desee examinar.

> **Tip**
>
> La página de detalles de la prueba de penetración muestra un resumen del estado de la prueba, la fecha de finalización y el número de hallazgos identificados.

Paso 2: Supervise el progreso de las pruebas

Realice un seguimiento del progreso de la prueba de penetración mediante el indicador de pasos.

1. Ubique el indicador de escalones horizontales debajo del encabezado de la página.
2. Revise el estado de cada fase de prueba:
   - Preflight: configuración inicial y comprobaciones de conectividad
   - Análisis estático: análisis de código y configuración
   - Pentests: pruebas en tiempo de ejecución y escaneo de vulnerabilidades
   - Finalización: validación final y generación de informes

> **Note**
>
> Cada paso muestra un indicador de estado (completo, en curso o pendiente). Los hallazgos se descubren y validan a lo largo del proceso de prueba, y aparecen nuevas vulnerabilidades a medida que se completa cada fase.

Paso 3: Dirígete a la pestaña de información general sobre la ejecución de la prueba de penetración

1. La sección Resumen de la ejecución proporciona el estado de la prueba, la duración y otros detalles de alto nivel. También proporciona un panel de control de los hallazgos de seguridad clasificados por nivel de gravedad y tipos de riesgo
2. La descripción general de la aplicación realizada por AWS Security Agent proporciona un resumen de la ejecución de la prueba de penetración
3. Los puntos de enlace descubiertos por el agente de seguridad de AWS proporciona una lista de todos los puntos de enlace descubiertos y probados por el agente de seguridad de AWS durante la ejecución de la prueba.

Paso 4: Diríjase a la pestaña de registros de las pruebas de penetración

Acceda a los registros detallados de todas las acciones que AWS Security Agent ejecutó durante la prueba preliminar.

1. Las acciones se clasifican por tipo de acción y tipos de riesgo.
2. Seleccione una acción específica para ver los registros detallados:
   - Resumen de las pruebas: High-level resumen de las acciones y los resultados del agente
   - Registros de pruebas de penetración: registros detallados de todas las actividades de prueba

> **Note**
>
> Las acciones del validador proporcionan registros que validan los hallazgos en cada categoría

> **Note**
>
> La pestaña Hallazgos muestra una vista dividida con la lista de hallazgos a la izquierda y los detalles de los hallazgos seleccionados a la derecha.

Paso 5: Navegue hasta los hallazgos

Cada hallazgo de la lista muestra información clave para ayudarle a evaluar rápidamente su importancia.

> **Note**
>
> Filtro de confianza predeterminado
>
> De forma predeterminada, solo se muestran los resultados con un nivel de confianza alto por parte del agente. Para mostrar también los resultados con un nivel de confianza medio o bajo por parte de los agentes y los falsos positivos, desactive la opción Ocultar los hallazgos no verificados.

Revisa la información que aparece en cada tarjeta de búsqueda:

- Nombre de búsqueda: el título y el identificador de la vulnerabilidad
- Distintivo de confianza: indica el nivel de confianza del agente en el hallazgo (alto, medio o bajo)
- Distintivo de gravedad: muestra el nivel de riesgo con un código de colores:
  - Crítico (rojo): requiere una acción inmediata; la explotación podría comprometer el sistema
  - Alto (rojo): requiere atención inmediata; la explotación podría tener un impacto significativo en la seguridad
  - Medio (naranja): debe abordarse en un plazo razonable; contribuye al riesgo general de seguridad

- Bajo (amarillo): se puede abordar como parte de un mantenimiento regular; el riesgo inmediato es mínimo
- Informativo (azul): con fines informativos; riesgo inmediato mínimo o nulo

- Fecha y hora de la última actualización: muestra cuándo se modificó o validó el hallazgo por última vez
- Vista previa de la descripción: breve resumen de la vulnerabilidad

> **Important**
>
> Priorice los hallazgos con distintivos de gravedad crítica o alta y niveles de confianza altos, ya que representan vulnerabilidades validadas que requieren una solución inmediata.

Paso 6: Revise los detalles de la búsqueda

Seleccione los hallazgos individuales para ver información completa sobre cada vulnerabilidad.

1. Seleccione el nombre de un hallazgo en el panel izquierdo para mostrar sus detalles en el panel derecho.
2. Revise el estado de la validación:

   > **Note**
   >
   > Si un hallazgo muestra el mensaje Desconocido «Este hallazgo aún no ha sido validado por AWS Security Agent», significa que la detección de la vulnerabilidad aún se está confirmando. Es posible que estos hallazgos requieran una verificación manual.

3. Revisa los atributos clave que aparecen en la parte superior:
   - Confianza del agente: el nivel de confianza que tiene AWS Security Agent en este hallazgo
   - Gravedad: el nivel de riesgo con una insignia codificada por colores
   - Búsqueda de registros: seleccione «Rastrear acciones y registros» para ver los registros de ejecución detallados y las pruebas
   - Tipo de riesgo: la categoría o el tipo de riesgo de seguridad (por ejemplo, omisión de autenticación o inyección de SQL)
4. Amplíe la sección de descripción para que diga:

- Una explicación detallada de la vulnerabilidad
- Cómo funciona la vulnerabilidad
- Por qué representa un riesgo de seguridad
- El impacto potencial en su aplicación

5. Amplíe la sección Razonamiento del riesgo para comprender el cálculo de la gravedad:
   - Desglose de las métricas del CVSS (Common Vulnerability Scoring System)
   - Vector de ataque (AV): cómo se puede explotar la vulnerabilidad
   - Complejidad del ataque (AC): qué tan difícil es el exploit
   - Privilegios requeridos (PR): ¿Qué nivel de acceso se necesita
   - Interacción con el usuario (UI): si es necesaria la acción del usuario
   - Ámbito (S): si la vulnerabilidad afecta a otros componentes
   - Impactos en la confidencialidad, la integridad y la disponibilidad
6. Amplíe la sección Pasos para reproducir para ver:
   - Pasos técnicos detallados para recrear la vulnerabilidad
   - Ejemplos de solicitud y respuesta
   - Parámetros o condiciones específicos que desencadenan el problema
7. La sección del script de verificación proporciona una forma ejecutable de reproducir el hallazgo. Amplíe esta sección (cuando esté disponible) para ver:
   - Instrucciones: cómo configurar y ejecutar el script de verificación
   - Variables de entorno: enumera las variables obligatorias que debe configurar antes de ejecutar el script. Los valores confidenciales están redactados por motivos de seguridad.
   - Descargar el script: elija descargar el script de verificación ejecutable

> **Note**
>
> Los scripts de verificación solo están disponibles para las vulnerabilidades confirmadas. El agente debe haber generado y validado correctamente un script de reproducción ejecutable.

> **Note**
>
> Los scripts de verificación se generan mediante IA generativa. Revise el script antes de ejecutarlo y ejecútelo solo en los sistemas que esté autorizado a probar. Para obtener orientación sobre cómo probar AI-generated los scripts de forma responsable, consulte la Política de IA responsable de AWS.

> **Tip**
>
> El script de verificación proporciona una forma ejecutable de reproducir el hallazgo de forma independiente. Defina las variables de entorno necesarias con sus propias credenciales y, a continuación, ejecute el script en el sistema de destino para confirmar la existencia de la vulnerabilidad.

> **Tip**
>
> Utilice el enlace «Rastrear acciones y registros» para acceder al paquete completo de pruebas, que incluye las solicitudes HTTP, las respuestas y los intentos de explotación que demuestran la vulnerabilidad.

Edite los hallazgos

Puede editar cualquier hallazgo para corregir sus detalles o afinar la evaluación del agente. Los siguientes campos se pueden editar:

- nombre: el título del hallazgo
- descripción: descripción detallada de la vulnerabilidad de seguridad
- estado: estado actual del hallazgo
- Tipo de riesgo: tipo de riesgo de seguridad identificado
- Nivel de riesgo: nivel de gravedad (crítico, alto, medio, bajo, informativo)
- RiskScore: puntuación de riesgo numérica
- razonamiento: justificación de la puntuación de riesgo asignada

- AttackScript: Proof-of-concept código que demuestra la vulnerabilidad
- Nota para el cliente: nota opcional en la que se explica el motivo de la modificación

Para editar un hallazgo:

1. Navegue hasta la página de detalles de la búsqueda.
2. Seleccione el icono de edición para modificar cualquiera de los campos de la lista anterior.
3. Guarde los cambios.

> **Note**
>
> Las modificaciones se guardan inmediatamente y se reflejan en el resultado. Si la personalización de hallazgos está habilitada, todos los campos editables que modifique se utilizarán para refinar las preferencias del agente para futuras ejecuciones.

Vea la versión original del agente

Al editar una búsqueda, aparece un selector de versiones en el encabezado de detalles de la búsqueda. Esto le permite ver la evaluación original del agente:

1. Localice el selector de versiones en el encabezado de detalles de búsqueda.
2. Seleccione Original para ver el hallazgo tal como lo produjo originalmente el agente.
3. Seleccione Más reciente para volver a la versión actual con las modificaciones aplicadas.

Revise los hallazgos personalizados

Cuando la personalización de hallazgos está habilitada, AWS Security Agent aprende de las modificaciones que realiza en las conclusiones. El agente aplica esas preferencias a hallazgos similares en futuras pruebas de penetración. Cuando se ha ajustado un resultado en función de tus ediciones anteriores, el panel de detalles muestra una sección de cambios de personalización. Para obtener información sobre cómo activar esta función, consulte Activar o desactivar la personalización de los resultados.

1. Localice la sección de cambios de personalización en el panel de detalles de búsqueda.

> **Note**
>
> La sección de cambios de personalización solo aparece cuando se descubre que AWS Security Agent ha alineado con sus ediciones anteriores. Los resultados que no coinciden con ninguna preferencia aprendida se muestran exactamente como los produjo el agente, sin esta sección.

2. Revise el resumen de lo que ha cambiado y por qué. El resumen enumera cada atributo ajustado con su valor original producido por el agente, el valor personalizado y el razonamiento. Por ejemplo:

Sobre la base de sus ediciones anteriores, se han introducido los siguientes cambios en el resultado obtenido originalmente por el sistema: el nivel de riesgo pasó de MEDIO a CRÍTICO; la puntuación de riesgo pasó de 5,3 a 9,5; razonamiento: se ha mejorado la gravedad para reflejar la exposición completa del código fuente de la aplicación a través de mapas fuente de acceso público.

1. Revise el resumen para comprender cómo se ajustó el hallazgo antes de decidir cómo actuar en consecuencia.
2. Para anular un resultado personalizado, edítelo de nuevo como lo haría con cualquier otro hallazgo (por ejemplo, cambie la gravedad o la puntuación de riesgo). La edición más reciente siempre tiene prioridad: AWS Security Agent aprende de ella y aplica la preferencia actualizada en la siguiente ejecución, sustituyendo a la regla anterior.

> **Note**
>
> Los cambios de personalización ajustan los atributos de búsqueda, como RiskLevel, RiskScore, nombre, descripción, razonamiento y AttackScript, para reflejar los estándares que AWS Security Agent aprendió de sus ediciones. Cualquier campo que haya editado anteriormente puede ajustarse en función de hallazgos similares en futuras ejecuciones.

Cómo aprende la personalización de tus ediciones

Cuando la personalización de hallazgos está habilitada, AWS Security Agent aprende de todas las modificaciones que realice en las conclusiones y aplica ajustes similares en futuras ejecuciones.

Todos los campos que edite (tal y como se indica en la sección anterior sobre cómo editar los resultados) se utilizarán para refinar las preferencias aprendidas por el agente.

> **Note**
>
> En el caso del campo de estado, solo se considera una preferencia que se puede aprender si se marca un hallazgo como FALSE_POSITIVE. Los cambios en otros valores de estado no activan el aprendizaje.

En la siguiente prueba, el agente evalúa los nuevos hallazgos en función de sus preferencias aprendidas y aplica los ajustes necesarios. Aparece una sección de cambios de personalización en cada resultado que se haya ajustado, en la que se explica lo que se ha modificado.

> **Note**
>
> La personalización solo se aprende de las modificaciones realizadas en la última tanda de pruebas completada. La función debe estar habilitada en el momento en que comience la prueba para que se produzca el aprendizaje. Si edita la misma conclusión más adelante, tendrá prioridad la edición más reciente: el agente actualizará sus preferencias para reflejar su última decisión.

Activa o desactiva la personalización de los resultados

La personalización de los resultados está habilitada de forma predeterminada. Para desactivarla o volver a activarla:

1. Navegue hasta su configuración de pentest.
2. Localice el botón de personalización de los hallazgos.
3. Para activar la personalización de los hallazgos, active el conmutador. Para desactivarlo, apáguelo.

Si está deshabilitada, los resultados aparecen en su estado original, producidos por el agente, sin que se aplique ninguna personalización. Las preferencias aprendidas anteriormente se conservan y se volverán a aplicar si se vuelve a activar la función.

Paso 7: Interprete las métricas del CVSS

Comprender las métricas del CVSS le ayuda a evaluar la verdadera gravedad y a priorizar los esfuerzos de remediación.

Al revisar la sección Razonamiento, preste atención a estas métricas clave:

- Vector de ataque (Network/Adjacent/Local/Physical): indica la distancia con la que se puede ejecutar el ataque
- Complejidad del ataque (Low/High): muestra si se requieren condiciones especializadas para explotarlo
- Privilegios requeridos (None/Low/High): identifica el nivel de acceso que necesita un atacante
- Interacción con el usuario (None/Required): determina si el exploit necesita la participación del usuario
- Confidentiality/Integrity/Availability Impacto (None/Low/High): mide el impacto en la seguridad del sistema

> **Important**
>
> Los hallazgos relacionados con el vector de ataque a la red, la baja complejidad y el alto confidentiality/integrity impacto representan las vulnerabilidades más peligrosas que requieren atención inmediata.

Paso 8: Priorizar y abordar los hallazgos

Tome medidas en función de los hallazgos para corregir las vulnerabilidades y mejorar la seguridad de su aplicación.

Para hallazgos críticos y de gravedad alta con un alto grado de confianza:

1. Revise la descripción y los pasos para reproducir las secciones en detalle.
2. Acceda a los registros detallados a través del enlace «Rastrear acciones y registros» para reunir pruebas completas.
3. Acceda a las correcciones de código listas para su implementación mediante uno de estos métodos:

- Para la corrección automática: usa el enlace de solicitud de cambios en la sección de remediación
- Para las solicitudes manuales: selecciona «Código de remediación» en la página de resultados para solicitar una solicitud de retirada. Requisitos previos:
- El administrador debe habilitar la corrección de código para GitHub los repositorios en la consola de AWS Security Agent
- Los repositorios deben estar incluidos en su configuración de pentest

4. Planifique una prueba de penetración de seguimiento para comprobar que la solución es eficaz.

Para hallazgos de gravedad media y baja:

1. Establezca prioridades en función de su tolerancia al riesgo y del contexto empresarial.
2. Incluya las tareas de remediación en su planificación habitual de los sprints de desarrollo.
3. Considere si varios hallazgos de baja gravedad juntos crean un mayor riesgo.
4. Documente cualquier riesgo aceptado con la justificación adecuada.

> **Important**
>
> No ignore los hallazgos de baja gravedad. A menudo, se pueden encadenar varias vulnerabilidades de baja gravedad para crear exploits más graves, especialmente cuando se combinan con la ingeniería social o el acceso físico.

Paso 9: Realice un seguimiento del progreso de la remediación

Utilice la interfaz de resultados para hacer un seguimiento de las vulnerabilidades que se han abordado y cuáles requieren medidas adicionales.

1. Mientras trabaja en la remediación, consulte la sección Pasos para reproducir para verificar las correcciones.
2. Documente su enfoque de remediación para cada hallazgo para futuras auditorías de referencia y cumplimiento.

> **Tip**
>
> Mantenga un registro de correcciones que asigne cada hallazgo a su resolución, incluidos los cambios de código, las actualizaciones de configuración o las decisiones arquitectónicas tomadas para abordar la vulnerabilidad.

Siguientes pasos

Tras revisar los resultados de la prueba de penetración:

- Priorice los hallazgos críticos y de alta gravedad con total confianza para una remediación inmediata
- Descargue, revise y ejecute los scripts de verificación en su entorno de prueba para probarlos e identificar las vulnerabilidades
- Cree tickets de seguimiento en su sistema de gestión de problemas con enlaces para encontrar detalles y pruebas
- Implemente correcciones y controles de seguridad para abordar las vulnerabilidades identificadas
- Supervise el indicador de progreso de la ejecución de la prueba de penetración para detectar las vulnerabilidades recién descubiertas
- Programe una prueba de penetración de seguimiento para verificar que las vulnerabilidades se hayan subsanado adecuadamente
- Actualice el proceso de pruebas de seguridad de las aplicaciones y el modelo de amenazas en función de los hallazgos
- Revise las métricas del CVSS para comprender el estado general de seguridad de su aplicación

Para obtener más información sobre la realización de pruebas de penetración, consultethe section called “Crea una prueba de penetración”.

Para obtener más información sobre cómo comprender el ciclo de vida de Security Agent, consultethe section called “Comprenda la jerarquía y el ciclo de vida de los recursos”.

Proporcione credenciales de autenticación para las pruebas de penetración

Proporcione credenciales para que AWS Security Agent pueda probar áreas autenticadas de sus aplicaciones web. Sin credenciales, el agente solo puede probar páginas y API de acceso público.

Configure las credenciales de autenticación

1. En el flujo de trabajo de creación de la prueba de penetración, busque la sección Credenciales de autenticación: opcionales.
2. En la sección Credencial #1, elija el método de introducción de credenciales:
   - Introduzca las credenciales: introduzca las credenciales directamente. Ideal para entornos de desarrollo y pruebas.
   - Configuración avanzada: utilice la administración de AWS-native credenciales. Se recomienda para entornos de producción y credenciales confidenciales.

Opciones avanzadas

Si selecciona la configuración avanzada, puede elegir entre tres estrategias de credenciales:

- Asunción del rol de IAM: para aplicaciones que utilizan la autenticación de AWS Cognito o IAM
- AWS Secrets Manager: para un almacenamiento seguro de credenciales con cifrado y rotación
- Función Lambda: para la generación dinámica de credenciales o flujos de autenticación complejos

Introduzca las credenciales directamente

1. Seleccione Introducir credenciales.
2. Introduzca el nombre de usuario y la contraseña.
3. En el menú desplegable URL de acceso, seleccione la URL en la que se utilizarán estas credenciales. Debe seleccionarse de la lista de puntos finales de destino.
4. (Opcional) En el campo 2FA (opcional), proporciona un secreto TOTP para las aplicaciones que requieren una autenticación de dos factores. Puede:
   - Introduzca el secreto TOTP directamente (por ejemplo,`JBSWY3DPEHPK3PXP`) o introduzca el `otpauth://totp/` URI completo (por ejemplo,). `otpauth://totp/Example:user@example.com?secret=JBSWY3DPEHPK3PXP&issuer=Example`
   - Selecciona el icono de carga para subir una imagen de código QR desde la página de configuración de la aplicación de autenticación. El código QR se escanea localmente y el URI del TOTP se extrae automáticamente.

Cuando se proporciona un secreto TOTP, el agente genera automáticamente códigos nuevos de un solo uso y los introduce cuando se detecta un mensaje de autenticación de dos factores durante el inicio de sesión.

5. (Opcional) Amplíe el mensaje de inicio de sesión de Agent Space para proporcionar instrucciones de inicio de sesión específicas si su aplicación tiene un flujo de autenticación complejo.

> **Important**
>
> Utilice cuentas de prueba con acceso representativo en lugar de cuentas personales o administrativas.

Utilice la configuración avanzada

Cuando selecciona una estrategia de credenciales avanzada (función Secrets Manager, Lambda o IAM), AWS Security Agent recupera sus credenciales directamente del recurso de AWS configurado mediante la función de servicio. Utilice el mensaje de inicio de sesión de Agent Space para proporcionarle al agente instrucciones sobre cómo aplicar esas credenciales a su aplicación, por ejemplo, a qué URL de inicio de sesión debe navegar y qué campos del formulario debe rellenar.

> **Note**
>
> Los secretos de Secrets Manager y las funciones de Lambda deben estar en la misma cuenta de AWS que la configuración de AWS Security Agent. Cross-account actualmente no se admiten las credenciales.

1. Seleccione Configuración avanzada.
2. En el menú desplegable Estrategia de acceso de usuarios, elige una de las siguientes opciones:

Seleccione el rol de IAM disponible para que lo asuma el agente

Utilice esta opción para las aplicaciones que utilizan AWS Cognito, API Gateway con autenticación de IAM u otros AWS-native sistemas de autenticación. La función de IAM debe tener una relación de confianza que permita a AWS Security Agent asumirla y tener permisos para acceder al sistema de autenticación de la aplicación.

Seleccione una credencial estática del AWS Secrets Manager conectado

Utilice esta opción para recuperar las credenciales de forma segura de AWS Secrets Manager mediante auditorías de cifrado, rotación y acceso.

El rol de IAM debe tener `secretsmanager:DescribeSecret` permisos `secretsmanager:GetSecretValue` y permisos.

El agente recupera el valor secreto directamente de Secrets Manager. Utilice el mensaje de inicio de sesión de Agent Space para indicarle al agente cómo aplicar esas credenciales al flujo de inicio de sesión de su aplicación, por ejemplo, a qué URL debe navegar y qué campos del formulario debe rellenar. Puedes usar cualquier formato para almacenar tu secreto, ya que el agente interpretará el formato siguiendo las instrucciones que proporciones en el mensaje de inicio de sesión.

Por ejemplo, si el agente va a enviar un formulario de inicio de username/password sesión ahttps://example.com/login, puedes formatear tu secreto como JSON con `password` campos `username` y. Si la aplicación requiere la TOTP-based autenticación de dos factores, incluye un `totpSecret` campo con el secreto del TOTP directamente o un URI completo`otpauth://totp/`:

```
{
  "username": "test-user",
  "password": "secure-password-here",
  "totpSecret": "JBSWY3DPEHPK3PXP"
}
```

A continuación, configure las instrucciones de autenticación:. Establezca la URL de acceso en `https://example.com` (o cualquier otra URL seleccionada de la lista de puntos finales de destino). Introduzca lo siguiente en el mensaje de inicio de sesión de Agent Space: «Navegue hasta el nombre de usuario https://example.com/login y la contraseña proporcionados e introdúzcalos en el formulario».

Como otro ejemplo, si en vez de eso tienes que incluir una clave de API en un encabezado HTTP, puedes guardarla como texto sin formato:

```
"api-key-here"
```

A continuación, configure las instrucciones de autenticación:. Introduzca lo siguiente en la línea de inicio de sesión de Agent Space: «Defina el X-API-Key encabezado con la clave de API proporcionada para todas las solicitudes».

> **Important**
>
> Solo se admite la TOTP-based autenticación de dos factores. No se admiten los SMS, el correo electrónico, las notificaciones push, las claves de hardware ni la autenticación OAuth.

Seleccione la función Lambda disponible para recuperar las credenciales de forma dinámica

Utilice esta opción para sistemas de autenticación complejos, generación dinámica de credenciales o integración con proveedores de identidad externos.

El rol de IAM debe tener `lambda:InvokeFunction` permisos y la función debe completarse en 30 segundos.

Cuando se ejecuta la prueba de penetración, AWS Security Agent invoca la función de AWS Lambda de forma sincrónica y supera un evento que identifica la prueba de penetración y la credencial específica que se está resolviendo:

```
{
  "pentest_arn": "arn:aws:securityagent:us-west-2:111122223333:pentest/pt-
abcd1234-5678-90ab-cdef-EXAMPLE11111",
  "actor_identifier": "Credential1"
}
```

- `pentest_arn`— El nombre del recurso de Amazon (ARN) de la prueba de penetración para la que se está resolviendo la credencial. Úselo para analizar, autorizar o auditar la solicitud dentro de su función.
- `actor_identifier`— El nombre de la credencial que asignó a esta credencial en la consola (por ejemplo,`Credential1`). Úselo para devolver la credencial correcta cuando una sola función sirva para varias credenciales.

El agente usa el resultado de la función directamente como credencial. Utilice el mensaje de inicio de sesión de Agent Space para indicarle al agente cómo aplicar esas credenciales a su aplicación, del mismo modo que lo haría con AWS Secrets Manager. Consulte los ejemplos the section called “Seleccione una credencial estática del AWS Secrets Manager conectado” de cómo formatear la salida de la función Lambda y los tipos de autenticación compatibles.

Configure varias credenciales

Para probar diferentes funciones de usuario o sistemas de autenticación:

1. Elija Añadir otra credencial.
2. Configure la credencial adicional mediante cualquiera de los dos métodos de entrada.
3. Para eliminar una credencial, elija Eliminar en la sección de credenciales.

Optimización para iniciar sesión

La optimización del inicio de sesión permite a AWS Security Agent aprender los patrones de navegación de ejecuciones anteriores de pentest y aplicarlos a ejecuciones posteriores. Estos patrones incluyen flujos de inicio de sesión y flujos de trabajo de autenticación de varios pasos. Esto reduce el tiempo que el agente dedica a volver a descubrir cómo autenticarse, lo que se traduce en escaneos más rápidos y en una cobertura de pruebas más uniforme.

Cómo funciona la optimización del inicio de sesión

En la primera prueba, el agente descubre cómo navegar por el flujo de inicio de sesión de la aplicación con las credenciales que usted proporciona. Registra los pasos de navegación correctos y genera un archivo de habilidades que captura el flujo de trabajo de inicio de sesión aprendido.

En las siguientes ejecuciones, el agente lee el archivo de habilidades guardado y aplica directamente el patrón de navegación aprendido, saltándose la fase de descubrimiento. Esto significa:

- Se agilizan las pruebas autenticadas: el agente aplica patrones de navegación comprobados de forma inmediata en lugar de explorar desde cero
- Comportamiento más coherente: el agente sigue el mismo camino comprobado en lugar de explorar alternativas

> **Note**
>
> La optimización del inicio de sesión aprende durante la primera sesión de inicio de sesión de una ejecución. Las siguientes sesiones de inicio de sesión de la misma ejecución se beneficiarán de lo aprendido en la primera sesión. En futuras ejecuciones, todas las sesiones de inicio de sesión se beneficiarán de la habilidad guardada.

Habilita o deshabilita la optimización del inicio de sesión

La optimización del inicio de sesión está habilitada de forma predeterminada. Para deshabilitarla o volver a habilitarla:

1. En la configuración de prueba actualizada, vaya a la sección Credenciales de autenticación: opcionales.
2. Localice el conmutador de optimización del inicio de sesión.
3. Para activar la optimización del inicio de sesión, activa el conmutador. Para deshabilitarlo, apáguelo.

Cuando está deshabilitado, el agente vuelve a descubrir el flujo de inicio de sesión desde cero en cada ejecución. Las habilidades de navegación adquiridas anteriormente se conservan y se volverán a aplicar si se vuelve a activar la función.

> **Tip**
>
> Si el flujo de inicio de sesión de la aplicación cambia significativamente (por ejemplo, una página de inicio de sesión rediseñada o un nuevo paso de autenticación), el agente se adapta automáticamente actualizando las habilidades adquiridas en la siguiente ejecución. No es necesario restablecer manualmente la optimización.

Solucionar el hallazgo de una prueba de penetración

Al ver los resultados de una prueba de penetración, puede solicitar a AWS Security Agent que intente corregir un hallazgo. En el caso de GitHub los repositorios privados, AWS Security Agent abre una solicitud de cambios con la solución propuesta. En el caso de los repositorios públicos, la corrección está disponible como un archivo diff descargable que puede aplicar localmente.

Debe habilitar la búsqueda de soluciones en la consola de administración de AWS. (Consulte the section called “Permita a los usuarios iniciar la corrección de los hallazgos de las pruebas de penetración y la revisión del código”). Los usuarios pueden iniciar la reparación de un hallazgo específico desde la aplicación web AWS Security Agent.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Una prueba de penetración completada o en curso
- Acceso a la aplicación web AWS Security Agent
- Familiaridad con la arquitectura y los requisitos de seguridad de su aplicación

Paso 1: Habilitar o deshabilitar la corrección automática

Puede configurar las opciones de corrección del código al crear o modificar una prueba de penetración. Si habilita la corrección automática, AWS Security Agent intentará corregir automáticamente los GitHub repositorios asociados si el agente confirma un hallazgo durante la última prueba. También puede iniciar manualmente la corrección del código. En la vista para editar los detalles de la prueba de penetración, en la sección Corrección automática de código, active o desactive la corrección de código.

Paso 2: Seleccione los repositorios para la corrección del código

1. Elija Siguiente hasta el último paso. Recursos de aprendizaje adicionales.
2. Elija Seleccionar entre los recursos.
3. Elige GitHub repositorios.
4. Seleccione los repositorios que desee para la corrección del código.
5. Guarde la prueba de penetración.
6. Puedes ver los repositorios asociados correctamente en la pestaña de recursos de aprendizaje de la prueba de penetración.

Paso 3: Iniciar una prueba de penetración y ver los resultados

Realice la prueba de penetración para detectar los hallazgos. Para obtener más información, consulte the section called “Revise los resultados de una prueba de penetración”.

Paso 4: Iniciar y ver la corrección del código

1. Navegue hasta el hallazgo.
2. Si ha activado la corrección automática de código, se iniciará una corrección de código una vez que AWS Security Agent confirme el hallazgo.
3. Si desea iniciar una corrección de código de forma manual, pulse el botón Corregir código.
4. En la sección de corrección de código de la búsqueda, puedes ver el estado de la corrección del código y los enlaces a las solicitudes de extracción de cambios. Si el GitHub repositorio

es público, la corrección del código está disponible como un archivo descargable en lugar de como una solicitud de extracción. Puedes ejecutar `git apply /path/to/code_remediation_changes.diff` para aplicar el cambio a tu repositorio de forma local.

Seguridad y referencia

Guía de seguridad, cuotas de servicio e historial documental de AWS Security Agent.

Seguridad en AWS Security Agent

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS Security Agent en la AWS nube. Esto incluye la infraestructura de servicios, los modelos de IA y los agentes de pruebas de penetración. Third-party los auditores prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los programas de AWS cumplimiento.
- Seguridad en la nube – las siguientes áreas son su responsabilidad:
  - Administración del acceso a AWS Security Agent mediante políticas y permisos de IAM
  - Proteger el contenido que proporciona al servicio, incluidos los documentos de diseño, los repositorios de código y las URL de las aplicaciones para las pruebas de penetración
  - Configurar qué repositorios y aplicaciones se supervisan
  - Revisar los hallazgos de seguridad proporcionados por el servicio y actuar en función de ellos
  - Proteja sus aplicaciones según la guía de remediación proporcionada
  - La confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar AWS Security Agent.

Consideraciones de seguridad para las pruebas de penetración asistidas por IA y agentes de seguridad de AWS

AWS Security Agent es un agente pionero que protege sus aplicaciones de forma proactiva durante todo el ciclo de vida del desarrollo en todos sus entornos. Realiza revisiones de seguridad automatizadas y personalizadas según sus requisitos, y los equipos de seguridad definen de forma centralizada los estándares que se validan automáticamente durante las revisiones. Security Agent realiza pruebas de penetración bajo demanda personalizadas para su aplicación, detectando y notificando los riesgos de seguridad verificados. Este enfoque amplía la experiencia en seguridad de sus aplicaciones para adaptarla a la velocidad de desarrollo y, al mismo tiempo, proporciona una cobertura de seguridad integral. Al integrar la seguridad desde el diseño hasta la implementación, ayuda a prevenir las vulnerabilidades de forma temprana y a gran escala.

Los equipos de seguridad definen los requisitos de seguridad de la organización una vez en la consola de AWS: bibliotecas de autorización aprobadas, estándares de registro y políticas de acceso a los datos. AWS Security Agent aplica automáticamente estos requisitos de seguridad durante todo el desarrollo, evaluando los documentos de arquitectura y el código en función de sus estándares y proporcionando orientación específica cuando detecta infracciones. De este modo, se garantiza una aplicación coherente de la seguridad en todos los equipos y se escalan las revisiones para adaptarlas a la velocidad de desarrollo.

Para la validación de la implementación, AWS Security Agent transforma las pruebas de penetración de un obstáculo periódico en una capacidad bajo demanda. Los equipos de seguridad proporcionan las URL de destino, los detalles de autenticación, el código fuente y la documentación. AWS Security Agent desarrolla una comprensión profunda de las aplicaciones y ejecuta cadenas de ataque sofisticadas para descubrir y validar las vulnerabilidades, lo que permite a los equipos realizar pruebas siempre que sea necesario.

Capacidades clave

AWS Security Agent ofrece funciones de seguridad integrales que abarcan todo el ciclo de vida del desarrollo.

Revisión de la seguridad del diseño

AWS Security Agent proporciona comentarios de seguridad a pedido sobre los documentos de diseño y evalúa el cumplimiento de los requisitos de seguridad de la organización antes de escribir el código. Los equipos de seguridad suben los documentos de diseño a través de la aplicación web, donde el agente los analiza en función de sus requisitos de seguridad y expone los resultados

con una guía de corrección. De este modo, las revisiones manuales, que duran varias horas, se convierten en análisis específicos, lo que permite a los equipos abordar los problemas de seguridad cuando la remediación es más eficaz.

Revisión de seguridad del código

AWS Security Agent analiza las solicitudes de cambios o el código cargado para detectar los requisitos de seguridad de la organización y los problemas de seguridad más comunes, como la falta de validación de entradas y los riesgos de inyección de SQL. El agente proporciona una guía de corrección directamente en su plataforma de repositorio de código. Los equipos de seguridad configuran los repositorios que van a monitorear, escalando la evaluación a todas las bases de código y, al mismo tiempo, supervisando los problemas críticos.

On-demand pruebas de penetración

AWS Security Agent ofrece pruebas de penetración bajo demanda que descubren y notifican vulnerabilidades de seguridad validadas mediante escenarios de ataque de varios pasos personalizados. AWS Security Agent despliega agentes de IA especializados que desarrollan el contexto de la aplicación a partir de la documentación y las credenciales proporcionadas y, a continuación, ejecutan cadenas de ataque sofisticadas para identificar vulnerabilidades complejas que las herramientas convencionales pasan por alto. Documenta los hallazgos con análisis de impacto, rutas de ataque reproducibles y correcciones de código listas para su implementación, lo que acelera las pruebas de penetración de semanas a horas y amplía la validación de toda su cartera de aplicaciones.

Preguntas frecuentes

Control de seguridad &

¿Cómo autentica AWS Security Agent y mantiene el acceso a los sistemas?

Las pruebas de penetración son la única capacidad de AWS Security Agent que puede autenticarse en el sistema de un usuario en tiempo de ejecución. El AWS Security Agent acepta credenciales en forma de credenciales de nombre de usuario y contraseña estáticas (almacenadas en Secrets Manager) o de un proveedor de credenciales (como una función Lambda) como configuración antes de iniciar la prueba con lápiz. Estas credenciales se utilizan para ejercer la funcionalidad normal del usuario system/application durante todo el ciclo de vida de la prueba con lápiz. Recomendamos a los usuarios que creen nuevas credenciales con permisos con el alcance adecuado para poder probarlas.

¿Pueden los usuarios controlar el alcance y la profundidad de las pruebas para evitar impactos no deseados en el sistema?

AWS Security Agent permite a los clientes seleccionar una categoría específica de vulnerabilidad para explorarla en un punto final. Los usuarios pueden especificar direcciones URL fuera del alcance para evitar que AWS Security Agent realice pruebas de penetración contra esos objetivos. https://docs.aws.amazon.com/securityagent/latest/userguide/perform-penetration-test.html

¿Puede el propio AWS Security Agent representar un riesgo para la seguridad?

A AWS Security Agent se le indica que detecte los riesgos de seguridad, pero que lo haga utilizando cargas útiles intencionadamente con un impacto mínimo (por ejemplo, extrayendo la versión de SQL en lugar de dejar caer una tabla cuando se descubre un ataque de inyección de SQL). AWS Security Agent también se limita a barreras deterministas para evitar comportamientos riesgosos, como crear una carga excesiva en la aplicación de destino. Mientras las medidas de protección estén implementadas, es posible que se produzcan interacciones lógicas empresariales no intencionadas o no obvias, por lo que siempre recomendamos realizar pruebas de penetración en un entorno de preproducción.

¿Qué datos recopila AWS Security Agent y dónde se almacenan?

AWS Security Agent permite a los usuarios cargar artefactos para proporcionar un contexto sobre la aplicación que se está probando. Para obtener más información sobre la protección de datos, consultethe section called “Protección de datos”. AWS Security Agent seleccionará automáticamente la región óptima dentro de su zona geográfica para procesar sus solicitudes de inferencia. Esto maximiza los recursos informáticos disponibles, la disponibilidad de los modelos y ofrece la mejor experiencia al cliente. Sus datos permanecerán almacenados únicamente en la región en la que se originó la solicitud; sin embargo, es posible que las solicitudes de entrada y los resultados de salida se procesen fuera de esa región. Todos los datos se transmitirán cifrados a través de la red segura de Amazon. Para obtener más información, consulte Inferencia entre regiones.

¿Qué controles existen para bloquear las pruebas no autorizadas realizadas en un punto final?

Los puntos finales que se especifiquen como direcciones URL de destino para las pruebas preliminares requerirán la validación del DNS o la validación del HTTP como medida de propiedad. AWS Security Agent solicitará al cliente que añada un registro TXT al DNS del punto final o mostrará una cadena de validación que devuelva una ruta HTTP como prueba de propiedad. Solo después de demostrar que es propietario, el usuario podrá realizar una prueba de registro. La red bloqueará las solicitudes a direcciones URL ajenas al objetivo y a las URL accesibles.

Los clientes son responsables de asegurarse de que cuentan con la autorización adecuada para probar todos los sistemas que puedan verse afectados por sus actividades de pruebas de penetración. Todo uso del AWS Security Agent debe cumplir con la Política de uso aceptable de AWS (https://aws.amazon.com/aup/).

¿Cómo bloquean y denuncian los usuarios cualquier abuso mediante AWS Security Agent?

AWS Security Agent supervisa continuamente las solicitudes y los intentos de acceso a las URL que se encuentran fuera de las URL de destino. Si se detecta un uso indebido, como el intento de utilizar AWS Security Agent para realizar pruebas no autorizadas en un punto de conexión de terceros, se cancelarán todas las pruebas adicionales que se estén realizando en la cuenta. Los clientes pueden ponerse en contacto con AWS Support o con el equipo de su cuenta de AWS para obtener ayuda.

¿AWS Security Agent puede reemplazar el flujo de trabajo de las pruebas con lápiz?

AWS Security Agent no es un servicio profesional de pruebas de penetración, por lo que recomendamos a los usuarios que integren AWS Security Agent en su flujo de trabajo de revisión de seguridad. AWS Security Agent puede proporcionar accesibilidad a las pruebas de penetración bajo demanda durante la fase de desarrollo del ciclo de vida del software, cuando la colaboración con profesionales de pentesting sería demasiado temprana, poco práctica o tendría que volver a evaluarse con demasiada frecuencia. Los profesionales de la seguridad pueden revisar los hallazgos de AWS Security Agent para validarlos, explicarlos o ampliarlos para incluir nuevos hallazgos novedosos (si existen).

¿Pueden los usuarios configurar un control de acceso basado en roles (RBAC) para los distintos miembros del equipo?

Sí. AWS Security Agent se integra con el AWS IAM Identity Center, lo que permite a los administradores gestionar a los miembros del equipo que pueden acceder a la aplicación web AWS Security Agent, que permite a los usuarios crear, gestionar y ver revisiones de diseño y pruebas preliminares.

Capacidades de prueba

¿Qué tipos de vulnerabilidades puede detectar AWS Security Agent?

AWS Security Agent detecta vulnerabilidades entre las 10 principales aplicaciones web de OWASP. AWS Security Agent proporciona tipos de riesgo específicos que puede incluir o excluir en las pruebas que se describen a continuación. Los hallazgos pueden surgir dentro de estas categorías de riesgo o a partir de hallazgos novedosos descubiertos al seguir las pistas de una combinación de estas categorías de riesgo.

- Carga arbitraria de archivos
  - La carga arbitraria de archivos confirma que la aplicación debería poder defenderse de los archivos falsos y maliciosos de manera que la aplicación y los usuarios estén seguros
- Inyección de código
  - Inyección de código es el término general para los tipos de ataque que consisten en inyectar código que luego es utilizado interpreted/executed por la aplicación
- Inyección de comandos
  - La inyección de comandos es un ataque en el que el objetivo es ejecutar comandos arbitrarios en el sistema operativo anfitrión a través de una aplicación vulnerable
- Cross-Site Secuencias de comandos (XSS)
  - Cross-Site Los ataques de secuencias de comandos (XSS) son un tipo de inyección en el que se inyectan scripts maliciosos en sitios web que, por lo demás, serían benignos y confiables
- Referencia insegura a objetos directos
  - Las referencias directas a objetos (IDOR) inseguras se producen cuando una aplicación proporciona acceso directo a los objetos en función de las entradas proporcionadas por el usuario
- Vulnerabilidades del token web JSON
  - Los JWT son una fuente común de vulnerabilidades, tanto en la forma en que se implementan en las aplicaciones como en las bibliotecas subyacentes
- Inclusión de archivos locales
  - La vulnerabilidad de inclusión de archivos permite a un atacante incluir un archivo, normalmente aprovechando los mecanismos de «inclusión dinámica de archivos» implementados en la aplicación de destino
- Recorrido de trayectoria
  - El ataque Path Traversal (también conocido como recorrido de directorios) tiene como objetivo acceder a los archivos y directorios que se almacenan fuera de la carpeta raíz de la web
- Escalación de privilegios
  - La escalada de privilegios se produce cuando un usuario tiene acceso a más recursos o funciones de los que normalmente se le permiten, y la aplicación debería haber evitado dicha elevación o cambios
- Server-Side Falsificación de solicitudes (SSRF)
  - Server-Side La falsificación de solicitudes (SSRF) se produce cuando el atacante puede abusar de la funcionalidad del servidor para leer o actualizar los recursos internos

- Server-Side Inyección de plantillas
  - Las vulnerabilidades de inyección de plantillas en el servidor (SSTI) se producen cuando las entradas del usuario se incrustan en una plantilla de forma insegura y provocan la ejecución remota de código en el servidor
- Inyección de SQL
  - El ataque de inyección SQL consiste en la inserción o «inyección» de una consulta SQL a través de los datos de entrada del cliente a la aplicación
- Entidad externa XML
  - El ataque a una entidad externa XML es un tipo de ataque contra una aplicación que analiza la entrada XML. Este ataque se produce cuando un analizador XML con una configuración débil procesa una entrada XML que contiene una referencia a una entidad externa

¿Qué métodos de autenticación admite AWS Security Agent?

AWS Security Agent admite métodos de autenticación comunes, incluidos OAuth y JWT. Para obtener más información, consulte la Documentación de .

¿Cómo gestiona AWS Security Agent la prevención de la limitación de velocidad y la denegación de servicio (DOS)?

AWS Security Agent tiene barreras para evitar que interrumpa o destruya los puntos de conexión que se están probando, incluido DOS. Cuenta con controles de velocidad internos para detectar y gestionar patrones de tráfico inesperados.

¿Puede AWS Security Agent probar las API REST y GraphQL?

Sí, AWS Security Agent puede probar los puntos de enlace de la API. Recomendamos a los clientes que proporcionen la documentación de las API como recursos de aprendizaje adicionales para que AWS Security Agent tenga un mejor contexto sobre la forma y la funcionalidad de cada API que se está probando.

¿Cómo pueden comprobar los usuarios que AWS Security Agent ha cubierto todos los puntos de enlace y la lógica de las aplicaciones fundamentales?

El agente de seguridad de AWS realizará primero una exploración exhaustiva de las aplicaciones de destino e intentará utilizarla con normalidad antes de intentar cualquier explotación. Esto le permite desarrollar una comprensión práctica de la aplicación en tiempo de ejecución y descubrir la lógica

y los puntos finales críticos de la aplicación. Dada su naturaleza estocástica, no se garantiza que AWS Security Agent descubra y pruebe todas las aplicaciones y puntos de enlace críticos para ninguna aplicación de destino. La aplicación web AWS Security Agent proporciona visibilidad de todos los puntos de enlace descubiertos y de las acciones realizadas en los registros de las pruebas de penetración.

Precisión y fiabilidad &

¿Cómo valida AWS Security Agent los hallazgos antes de informar?

AWS Security Agent utiliza validadores deterministas para ayudar a validar el hallazgo informado. En los tipos de riesgo en los que no es posible utilizar validadores deterministas, AWS Security Agent reproducirá de forma independiente los pasos de búsqueda para aumentar la confianza en la validez de la conclusión. AWS Security Agent solo informa de los hallazgos de confianza alta o media y oculta los hallazgos no verificados de forma predeterminada.

¿Puede AWS Security Agent adaptarse a la lógica de las aplicaciones personalizadas?

De forma opcional, AWS Security Agent acepta el código fuente, el modelo de amenazas, los documentos de diseño y la documentación de la API como recursos de aprendizaje adicionales para obtener un contexto dirigido al usuario sobre la aplicación de destino utilizada en el ciclo de vida de una prueba preliminar.

¿Pueden los usuarios revisar la metodología de pruebas de AWS Security Agent antes de la ejecución?

Actualmente, no hay forma de obtener una vista previa del curso de acción de AWS Security Agent. El plan de agentes de seguridad de AWS es de naturaleza dinámica y se basa en la exploración de la aplicación de destino. Los clientes pueden monitorear AWS Security Agent durante su exploración en tiempo real observando los registros de las pruebas de penetración. Si los registros muestran una trayectoria no válida o no deseada, los clientes pueden interrumpir la ejecución de las pruebas de penetración en curso.

Implementación de la integración &

¿AWS Security Agent se integra con herramientas de seguridad (SIEM, gestión de vulnerabilidades) o CI/CD canalizaciones?

AWS Security Agent no se integra con ninguna herramienta o canal de seguridad CI/CD existente.

¿Cómo gestiona AWS Security Agent las configuraciones específicas del entorno?

AWS Security Agent se puede configurar para que se ejecute con funciones de IAM específicas, dentro de las VPC, con credenciales relevantes para la aplicación especificadas por el cliente y con los repositorios fuente de Github como referencia de código fuente para la aplicación de destino.

¿Puede AWS Security Agent ejecutarse en entornos aislados o aislados?

AWS Security Agent se puede configurar para que tenga conectividad con las VPC, incluidas las que no tienen acceso saliente a Internet.

¿Pueden varios miembros del equipo realizar pruebas simultáneamente?

AWS Security Agent admite 5 ejecuciones simultáneas de pentest por cuenta, independientemente de quién inicie la prueba. Los clientes pueden crear un máximo de 100 espacios de agentes y 1000 proyectos de Pentest.

Impacto operativo

¿Cuál es el impacto en el rendimiento de los sistemas probados?

AWS Security Agent tiene barandas para evitar que interrumpa o destruya los puntos de conexión que se están probando. Esto incluye controles de velocidad en la cantidad de llamadas que AWS Security Agent puede realizar a un punto final. Se espera que el sistema o el punto final que se esté probando aumente un poco el tráfico y que se activen posibles alertas de monitoreo debido a la actividad de la prueba con el lápiz. Nuestra recomendación es ejecutar únicamente AWS Security Agent o cualquier actividad de prueba con lápiz en un entorno de preproducción.

¿Los usuarios pueden programar o limitar AWS Security Agent?

AWS Security Agent no tiene API públicas ni la capacidad de programar las pruebas con lápiz. AWS Security Agent tampoco ofrece un control de simultaneidad de las solicitudes al punto final de destino al iniciar la ejecución de la prueba con lápiz. Si AWS Security Agent está causando problemas en los puntos de enlace de destino, los clientes pueden detener las pruebas preliminares en curso.

¿Cuál es la duración habitual de una evaluación de seguridad completa?

El tiempo de ejecución de cada prueba preliminar depende del alcance de la aplicación de destino y de los tipos de riesgo configurados para evaluarlos. La mayoría de las pruebas preliminares se completan en 16 horas.

Políticas administradas por AWS para los agentes de seguridad de AWS

Una política administrada por AWS es una política independiente creada y administrada por AWS. Las políticas administradas de AWS están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y roles.

Tenga en cuenta que es posible que las políticas administradas por AWS no otorguen permisos de privilegios mínimos para sus casos de uso específicos, ya que están disponibles para que los usen todos los clientes de AWS. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puede cambiar los permisos definidos en las políticas gestionadas por AWS. Si AWS actualiza los permisos definidos en una política administrada por AWS, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. Lo más probable es que AWS actualice una política gestionada por AWS cuando se lance un nuevo servicio de AWS o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte las políticas administradas por AWS en la Guía del usuario de IAM.

Política gestionada por AWS: SecurityAgentWebAppAPIPolicy

Otorga permisos para interactuar con la API de la aplicación web Security Agent. Esta política permite a los usuarios configurar y ejecutar pruebas de penetración de seguridad automatizadas, gestionar la ejecución de las pruebas, ver los resultados de seguridad y acceder a los recursos de Security Agent. Esta política hace referencia al tipo de recurso de la instancia de agente antigua y a las acciones específicas de IAM heredadas.

Detalles de los permisos

Esta política otorga permisos para interactuar con el servicio de control de pruebas de seguridad (securityagent: *) para:

- Pentest Management: cree, actualice, elimine y enumere las pruebas de penetración y sus trabajos de ejecución
- Hallazgos de seguridad: vea, describa y actualice los hallazgos de seguridad de las pruebas completadas, incluidos el contenido y los metadatos relacionados.
- Administración de tareas: enumere y recupere las tareas de revisión del código y de la documentación

- Descubrimiento de recursos: enumere y visualice las instancias de los agentes, los artefactos, las integraciones y los puntos finales descubiertos
- Ejecución de pruebas: inicie y detenga las ejecuciones de pruebas preliminares con funciones de monitoreo en tiempo real
- Corrección del código: inicie la corrección automática del código para detectar problemas de seguridad

Para ver la versión más reciente del documento de política de JSON, consulte SecurityAgentWebAppAPIPolicyla Guía de referencia de políticas administradas de AWS.

Política gestionada por AWS: AWSSecurityAgentWebAppPolicy

Otorga permisos para interactuar con la API de la aplicación web Security Agent. Esta política permite a los usuarios configurar y ejecutar pruebas de penetración de seguridad automatizadas, gestionar la ejecución de las pruebas, ver los resultados de seguridad y acceder a los recursos de Security Agent.

Detalles de los permisos

Esta política otorga permisos para interactuar con el servicio Security Testing Control (securityagent:*) para:

- Pentest Management: cree, actualice, elimine y enumere las pruebas de penetración y sus trabajos
- Hallazgos de seguridad: vea, describa y actualice los hallazgos de seguridad de las pruebas completadas, incluidos el contenido y los metadatos relacionados.
- Administración de tareas: enumere y recupere las tareas de revisión del código y del diseño
- Descubrimiento de recursos: enumere y visualice los espacios de los agentes, los artefactos, las integraciones y los puntos finales descubiertos
- Ejecución de pruebas: inicie y detenga los trabajos de prueba pendientes con funciones de monitoreo en tiempo real
- Remediación del código: inicie la corrección automática del código para detectar problemas de seguridad

Para ver la versión más reciente del documento de política de JSON, consulte AWSSecurityAgentWebAppPolicyla Guía de referencia de políticas administradas de AWS.

Los agentes de seguridad de AWS actualizan las políticas administradas por AWS

Consulte los detalles sobre las actualizaciones de las políticas administradas por AWS para los agentes de seguridad de AWS desde que este servicio comenzó a rastrear estos cambios.

Para recibir notificaciones de todos los cambios en el archivo de origen de esta página de documentación específica, puede suscribirse a la siguiente URL con un lector de RSS:

Cambio	Descripción	Fecha
Se agregaron permisos a AWSSecurityAgentWebAppPolicy.	Se agregaron permisos `TargetDomain` y `DesignReviewFeedback` recursos para los nuevos tipos de recursos.	31 de marzo de 2026
Se agregó una nueva política gestionada AWSSecurityAgentWebAppPolicy.	Se agregó una política administrada `AWSSecurityAgentWebAppPolicy` para el nuevo tipo de AgentSpace recurso y los cambios en el nombre de las acciones de IAM.	9 de febrero de 2026
Se agregaron permisos a SecurityAgentWebApAPIPolicy.	Se agregó `securityagent:StartCodeRemediation` para permitir a los usuarios iniciar la corrección automática del código en caso de problemas de seguridad.	20 de enero de 2026
Se agregaron permisos a SecurityAgentWebApAPIPolicy.	Se agregó `securityagent:BatchGetSecurityTestContentMetadata` para permitir a los usuarios ver imágenes en la consola.	5 de diciembre de 2025

Cambio	Descripción	Fecha
Los agentes de seguridad de AWS comenzaron a rastrear los cambios.	Los agentes de seguridad de AWS comenzaron a rastrear los cambios en sus políticas administradas por AWS.	2 de diciembre de 2025

Protección de datos en AWS Security Agent

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos en AWS Security Agent. Tal y como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También es responsable de las tareas de configuración y administración de la seguridad de los servicios de AWS que utilice. Para obtener información sobre la protección de datos en Europa, consulte la entrada del blog sobre el modelo de responsabilidad compartida de AWS y el RGPD en el blog sobre seguridad de AWS. Con fines de protección de datos, le recomendamos que proteja las credenciales de las cuentas de AWS y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con los recursos de AWS. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail rutas para capturar las actividades de AWS, consulte Trabajar con CloudTrail rutas en la Guía del CloudTrail usuario de AWS.
- Utilice las soluciones de cifrado de AWS junto con todos los controles de seguridad predeterminados dentro de los servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión FIPS. Para obtener

más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con AWS Security Agent u otros servicios de AWS mediante la consola, la API, la CLI de AWS o los SDK de AWS. Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

AWS Security Agent cifra todos los datos en reposo mediante claves de AWS-managed cifrado de forma predeterminada. Esto incluye:

- Documentos de diseño y código: todos los documentos de diseño, los repositorios de códigos y los artefactos de aplicaciones que proporcione para las revisiones de seguridad se cifran mediante AES-256 cifrado.
- Hallazgos de seguridad: todos los hallazgos de seguridad, los informes de vulnerabilidad y las recomendaciones de corrección están cifrados en reposo.
- Datos de configuración: los requisitos de seguridad, las políticas personalizadas y las configuraciones de los servicios están cifrados.
- Registros de auditoría: todos los registros de actividad del servicio y las pistas de auditoría están cifrados.

AWS Security Agent usa AWS Key Management Service (AWS KMS) para administrar las claves de cifrado. Si lo desea, puede utilizar una clave administrada por el cliente para cifrar sus datos, lo que le proporciona un control total sobre las claves de cifrado que protegen sus recursos. Para obtener más información, consulte the section called “Claves administradas por el cliente”.

Cifrado en tránsito

AWS Security Agent cifra todos los datos en tránsito mediante Transport Layer Security (TLS) 1.2 o una versión superior. Esto se aplica a:

- Comunicaciones de API: todas las llamadas a la API entre sus aplicaciones y AWS Security Agent utilizan HTTPS con cifrado TLS.
- Acceso a la consola: se accede a la consola de AWS Security Agent a través de HTTPS.
- Conexiones a repositorios: las conexiones GitHub y otros repositorios de código utilizan protocolos cifrados.
- Comunicaciones con los agentes: todas las comunicaciones entre el servicio AWS Security Agent y los agentes de pruebas de penetración utilizan canales cifrados.

Administración de claves

AWS Security Agent usa AWS Key Management Service (AWS KMS) para administrar las claves de cifrado. De forma predeterminada, los datos se cifran mediante AWS-managed claves. Si lo desea, puede especificar una clave gestionada por el cliente al crear recursos como espacios de agentes e integraciones. Para obtener más información, consulte the section called “Claves administradas por el cliente”.

Privacidad del tráfico entre redes

AWS Security Agent utiliza la Internet pública para comunicarse con los proveedores de control de código fuente alojados en la nube (GitHub GitLab, Bitbucket) y con Confluence Cloud.

En el caso de los proveedores autohospedados (GitLab Self-Managed GitHub Enterprise Server), puede configurar las conexiones privadas mediante Amazon VPC Lattice para mantener todo el tráfico dentro de la red de AWS. Para obtener más información, consulte the section called “Conéctese al control de código fuente alojado de forma privada”.

En la configuración predeterminada, AWS Security Agent utiliza la Internet pública para acceder a la aplicación y realizar pruebas de penetración. Si lo desea, puede configurar las pruebas de penetración para usar una VPC para acceder a su aplicación. Para obtener más información, consulte the section called “Conectar el agente a los recursos de VPC privados”.

Cross-Region procesamiento de datos

AWS Security Agent utiliza la inferencia entre regiones para optimizar los recursos informáticos disponibles y la disponibilidad del modelo. Según la región en la que se origine la solicitud, es posible que procesemos las solicitudes de entrada y los resultados de salida en una región diferente.

- En EE.UU. Este (Norte de Virginia) —`us-east-1`, EE.UU. Oeste (Oregón) —`us-west-2`, Asia Pacífico (Sídney) —`ap-southeast-2`, Asia Pacífico (Tokio) —`ap-northeast-1`, Europa

(Fráncfort) — `eu-central-1` y Europa (Irlanda) `eu-west-1` —, AWS Security Agent utiliza la inferencia geográfica entre regiones. Para la mayoría de las funciones, el procesamiento de datos permanece dentro del límite geográfico (como EE. UU., UE, Australia o Japón) en el que se originó la solicitud. En el caso de la corrección del código, las solicitudes de Australia y Japón se tramitan en la Unión Europea. Para obtener detalles de enrutamiento específicos de cada función, consulte la tabla de inferencias entre regiones.

- En Asia Pacífico (Bombay)`ap-south-1`, Asia Pacífico (Singapur) `ap-southeast-1` y Sudamérica (São Paulo)`sa-east-1`, AWS Security Agent utiliza la inferencia global entre regiones. Es posible que procesemos las solicitudes de entrada y los resultados de salida en cualquier región comercial de AWS.

En todos los casos, sus datos permanecen almacenados únicamente en la región en la que se originó la solicitud. Todos los datos transmitidos durante las operaciones entre regiones permanecen en la red de AWS y no atraviesan la Internet pública. Encriptamos los datos en tránsito entre las regiones de AWS.

Cross-Region La inferencia siempre está habilitada y no puede excluirse de ella. Para obtener más información sobre las regiones que procesan las solicitudes de cada función, consulte la sección Inferencia entre regiones de. the section called “Prácticas recomendadas de seguridad”

Eliminación de datos

Al eliminar datos de AWS Security Agent:

- Los datos están marcados para su eliminación y ya no se puede acceder a ellos a través del servicio.
- Los datos se eliminan de todos los sistemas de AWS Security Agent en un plazo de 30 días.

Para eliminar sus datos

1. En la consola de AWS, vaya a AWS Security Agent.
2. Elija los datos que desee eliminar (revisiones de seguridad, hallazgos o requisitos personalizados).
3. Para confirmar la eliminación, seleccione Eliminar.

Administración de identidades y accesos para AWS Security Agent

AWS Identity and Access Management (IAM) es una Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. IAM los administradores controlan quién puede autenticarse (iniciar sesión) y quién está autorizado (tiene permisos) para usar los recursos de AWS Security Agent. IAM es una Servicio de AWS que puede utilizar sin coste adicional.

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realice en AWS Security Agent.

Usuario del servicio: si utiliza el servicio AWS Security Agent para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más funciones de AWS Security Agent para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador.

Si no puede acceder a una función de AWS Security Agent, consultethe section called “Solución de problemas de identidad y acceso de AWS Security Agent”.

Administrador de servicios: si está a cargo de los recursos de AWS Security Agent en su empresa, probablemente tenga acceso total a AWS Security Agent. Es su trabajo determinar a qué funciones y recursos de AWS Security Agent deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM AWS Security Agent, consultethe section called “Cómo funciona AWS Security Agent con IAM”.

IAM administrador: si es IAM administrador, puede que le interese obtener información sobre cómo redactar políticas para administrar el acceso a AWS Security Agent. Para ver ejemplos de políticas basadas en la identidad de AWS Security Agent que puede utilizar IAM, consulte. the section called “Ejemplos de políticas basadas en la identidad de AWS Security Agent”

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario raíz de la cuenta de AWS Usuario de IAM, o debe asumir un IAM rol. AWS sugiere utilizar una función de IAM y evitar utilizar directamente al usuario root.

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center (IAM Identity Center) los usuarios, la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accede AWS mediante la federación, asume indirectamente un rol.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión en su cuenta de AWS AWS, consulte Cómo iniciar sesión en su cuenta de AWS en la Guía del Sign-In usuario de AWS.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte el proceso de firma de la versión 4 de Signature en la Referencia general de AWS.

Independientemente del método de autenticación que utilice, es posible que también deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte la Multi-factor autenticación en la Guía del usuario de AWS IAM Identity Center (sucesor de AWS Single Sign-On) y el uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Usuario raíz de la cuenta de AWS

Cuando crea una por primera vez Cuenta de AWS, comienza con una identidad de inicio de sesión única que tiene acceso completo a todos los Servicios de AWS recursos de la cuenta. Esta identidad recibe el nombre de usuario raíz de la cuenta de AWS y para obtener acceso a ella se inicia sesión con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja sus credenciales de usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía de referencia de administración de cuentas.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidad para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios empresarial, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener información sobre el Centro de identidades de IAM, consulte ¿Qué es el Centro de identidades de IAM? en la guía del usuario de AWS IAM Identity Center (sucesor de AWS Single Sign-On).

Usuarios de IAM y grupos

Una Usuario de IAMes una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, te recomendamos Usuarios de IAM que utilices credenciales temporales en lugar de crearlas con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales de larga duración Usuarios de IAM, le recomendamos que rote las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un IAM grupo es una identidad que especifica una colección de Usuarios de IAM. No puede iniciar sesión como grupo. Puede usar grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede tener un grupo denominado IAMAdmins y concederle permisos para administrar los recursos. IAM

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un rol Usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

IAM roles

Un IAM rol es una identidad dentro de ti Cuenta de AWS que tiene permisos específicos. Es similar a un Usuario de IAM, pero no está asociado a una persona específica. Puede asumir temporalmente un IAM rol en el AWS Management Console cambiando de rol. Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para obtener más información sobre los métodos de uso de roles, consulte Uso de IAM roles en la Guía del usuario de IAM.

IAM los roles con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información sobre los conjuntos de permisos, consulte los conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center (sucesor de AWS Single Sign-On).
- Usuario de IAM Permisos temporales: un usuario Usuario de IAM puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- Cross-account acceso: puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso a varias cuentas. Sin embargo, con algunos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso entre cuentas, consulte En qué se diferencian las IAM funciones de las políticas basadas en recursos en la Guía del usuario de IAM.
- Cross-service acceso: algunos utilizan funciones en otros. Servicios de AWS Servicios de AWS Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones Amazon EC2 o almacene objetos en él Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado a un servicio.
  - Permisos principales: cuando utilizas un rol Usuario de IAM o para realizar acciones en AWSél, se te considera principal. Las políticas conceden permisos a una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. En este caso, debe tener permisos para realizar ambas acciones.

  - Función de servicio: una función de servicio es una IAM función que asume un servicio para realizar acciones en tu nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentro IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Service-linked rol: un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir la función de realizar una acción en su nombre. Service-linked las funciones aparecen en su nombre Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver, pero no editar, los permisos de los roles vinculados al servicio.
- Aplicaciones en ejecución Amazon EC2 : puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una Amazon EC2 instancia y que realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la Amazon EC2 instancia. Para asignar un AWS rol a una Amazon EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la Amazon EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Uso de un IAM rol para conceder permisos a las aplicaciones que se ejecutan en Amazon EC2 instancias en la Guía del usuario de IAM.

Para saber si se deben usar IAM roles, consulte Cuándo crear un IAM rol (en lugar de un usuario) en la Guía del usuario de IAM.

Administración del acceso con políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos de las políticas determinan si la solicitud está permitida o denegada. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

Todas las IAM entidades (usuarios o roles) comienzan sin permisos. De forma predeterminada, los usuarios no pueden hacer nada, ni siquiera cambiar su propia contraseña. Para conceder permiso

a un usuario para hacer algo, el administrador debe asociar una política de permisos a un usuario. O bien el administrador puede agregar al usuario a un grupo que tenga los permisos necesarios. Cuando un administrador concede permisos a un grupo, todos los usuarios de ese grupo obtienen los permisos.

IAM las políticas definen los permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Identity-based políticas

Identity-based las políticas son documentos de política de permisos de JSON que puedes adjuntar a una identidad Usuario de IAM, como un rol o un grupo. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener información sobre cómo crear una política basada en la identidad, consulte Creación de IAM políticas en la Guía del usuario de IAM.

Identity-based las políticas se pueden clasificar además como políticas integradas o políticas gestionadas. Las políticas integradas están integradas directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y funciones de su empresa. Cuenta de AWS Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Resource-based políticas

Resource-based las políticas son documentos de políticas de JSON que se adjuntan a un recurso, como un Amazon S3 bucket. Los administradores de servicios pueden usar estas políticas para definir qué acciones puede realizar un responsable específico (miembro de la cuenta, usuario o rol) en ese recurso y en qué condiciones. Resource-based las políticas son políticas integradas. No existen políticas basadas en recursos que sean administradas.

Listas de control de acceso (ACL)

Las políticas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON. Amazon S3

AWS WAF, y Amazon VPC son ejemplos de servicios que admiten las ACL. Para obtener más información sobre las ACL, consulte Información general sobre la Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (Usuario de IAM o función). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y sus límites de permisos. Resource-based las políticas que especifican el usuario o el rol en el `Principal` campo no están limitadas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anula la autorización. Para obtener más información sobre los límites de los permisos, consulte los límites de los permisos para IAM las entidades en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada usuario raíz de la cuenta de AWS. Para obtener más información acerca de Organizaciones y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidad del rol y las políticas de la sesión. Los permisos también pueden proceder de una política basada en recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud

cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona AWS Security Agent con IAM

Antes de administrar el acceso IAM a AWS Security Agent, infórmese sobre IAM las funciones disponibles para su uso con AWS Security Agent.

Característica de IAM	Soporte para AWS Security Agent
the section called “Identity-based políticas para AWS Security Agent”	Sí
the section called “Resource-based políticas dentro de AWS Security Agent”	No
the section called “Acciones políticas para AWS Security Agent”	Sí
the section called “Recursos de políticas para AWS Security Agent”	Parcial
the section called “Claves de condición de política para AWS Security Agent”	Sí
the section called “Listas de control de acceso (ACL) en AWS Security Agent”	No
the section called “Attribute-based control de acceso (ABAC) con AWS Security Agent”	No
the section called “Uso de credenciales temporales con AWS Security Agent”	Sí
the section called “Sesiones de acceso directo para AWS Security Agent”	Sí
the section called “Funciones de servicio para AWS Security Agent”	No

Característica de IAM	Soporte para AWS Security Agent
the section called “Service-linked funciones de AWS Security Agent”	Sí

Para obtener una visión general de cómo Servicios de AWS funcionan AWS Security Agent y otros IAM, consulte Servicios de AWS ese trabajo IAM en la Guía del usuario de IAM.

Identity-based políticas para AWS Security Agent

Compatibilidad con las políticas basadas en identidad: sí

Identity-based las políticas son documentos de política de permisos de JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas IAM basadas en la identidad, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre todos los elementos que se utilizan en una política de JSON, consulte la referencia sobre los elementos de la política de IAM JSON en la Guía del usuario de IAM.

Identity-based ejemplos de políticas para AWS Security Agent

Para ver ejemplos de políticas de AWS Security Agent basadas en la identidad, consulte. the section called “Ejemplos de políticas basadas en la identidad de AWS Security Agent”

Resource-based políticas dentro de AWS Security Agent

Admite políticas basadas en recursos: no

Resource-based las políticas son documentos de política JSON que se adjuntan a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad

principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o servicios de AWS.

Para habilitar el acceso entre cuentas, puedes especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso están en cuentas de AWS distintas, un administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte el tema Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones políticas para AWS Security Agent

Soporta acciones Sí

Los administradores pueden usar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El `Action` elemento de una política IAM basada en la identidad describe la acción o las acciones específicas que la política permitirá o denegará. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. La acción se utiliza en una política para otorgar permisos para realizar la operación asociada.

Las acciones políticas en AWS Security Agent utilizan el siguiente prefijo antes de la acción:`securityagent:`. Por ejemplo, para conceder permiso a alguien para crear un entorno con la operación de la `CreateEnvironment` API de AWS Security Agent, debe incluir la `securityagent:CreateEnvironment` acción en su política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. AWS Security Agent define su propio conjunto de acciones que describen las tareas que puede realizar con este servicio.

Para especificar varias acciones en una única instrucción, sepárelas con comas del siguiente modo:

```
"Action": [
      "securityagent:action1",
      "securityagent:action2"
```

Puede utilizar caracteres comodín para especificar varias acciones (*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra `List`, incluya la siguiente acción:

```
"Action": "securityagent:List*"
```

Recursos de políticas para AWS Security Agent

Admite recursos de políticas: en forma parcial

Los administradores pueden usar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter asterisco (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Algunas acciones de la API de AWS Security Agent admiten varios recursos. Por ejemplo, se puede hacer referencia a varios entornos al solicitar la acción de la `ListEnvironments` API. Para especificar varios recursos en una única instrucción, separe los ARN con comas.

```
"Resource": [
      "EXAMPLE-RESOURCE-1",
      "EXAMPLE-RESOURCE-2"
```

Por ejemplo, el recurso del entorno AWS Security Agent tiene el siguiente ARN:

```
arn:${Partition}:securityagent:${Region}:${Account}:environment/${EnvironmentId}
```

Para especificar los entornos `my-environment-1` y `my-environment-2` en su declaración, utilice los siguientes ARN de ejemplo:

```
"Resource": [
```

```
        "arn:aws:securityagent:us-east-1:123456789012:environment/my-environment-1",
        "arn:aws:securityagent:us-east-1:123456789012:environment/my-environment-2"
```

Para especificar todos los entornos que pertenecen a una cuenta específica, utilice el comodín (*):

```
"Resource": "arn:aws:securityagent:us-east-1:123456789012:environment/*"
```

Claves de condición de política para AWS Security Agent

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El `Condition` elemento (o `Condition` bloque) le permite especificar las condiciones en las que entra en vigor una declaración. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una sola clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un Usuario de IAM permiso para acceder a un recurso solo si está etiquetado con su Usuario de IAM nombre. Para obtener más información, consulte los elementos IAM de la política: variables y etiquetas en la Guía del usuario de IAM.

AWS Security Agent define su propio conjunto de claves de condición y también admite el uso de algunas claves de condición globales. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Listas de control de acceso (ACL) en AWS Security Agent

Compatibilidad con ACL: no

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Attribute-based control de acceso (ABAC) con AWS Security Agent

Compatibilidad con ABAC (etiquetas en las políticas): no

Uso de credenciales temporales con AWS Security Agent

Compatibilidad con credenciales temporales: sí

Algunos servicios de AWS no funcionan cuando se inicia sesión con credenciales temporales. Para obtener información adicional, incluidos los servicios de AWS que funcionan con credenciales temporales, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en la consola de administración de AWS mediante cualquier método, excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accede a AWS mediante el enlace de inicio de sesión único (SSO) de su empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puede crear credenciales temporales manualmente mediante la AWS CLI o la API de AWS. A continuación, puede usar esas credenciales temporales para acceder a AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para AWS Security Agent

Admite sesiones de acceso directo (FAS): sí

Cuando utiliza un usuario o un rol de IAM para realizar acciones en AWS, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama a un servicio de AWS, junto con los del servicio de AWS solicitante, para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros servicios o recursos de AWS para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Funciones de servicio para AWS Security Agent

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puedes crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear un rol para delegar permisos a un servicio de AWS en la Guía del usuario de IAM.

Service-linked funciones de AWS Security Agent

Compatible con roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un servicio de AWS. El servicio puede asumir la función de realizar una acción en su nombre. Service-linked los roles aparecen en su cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Ejemplos de políticas basadas en la identidad de AWS Security Agent

De forma predeterminada, Usuarios de IAM los roles no tienen permiso para crear o modificar los recursos de AWS Security Agent. Tampoco pueden realizar tareas mediante la AWS API AWS Management Console AWS CLI, o. IAM El administrador debe crear IAM políticas que concedan permiso a los usuarios y a los roles para realizar operaciones de API específicas en los recursos específicos que necesitan. A continuación, el administrador debe adjuntar esas políticas a los grupos Usuarios de IAM o grupos que requieran esos permisos.

Para obtener información sobre cómo crear una política de IAM basada en la identidad utilizando estos ejemplos de documentos de política de JSON, consulte Creación de políticas mediante el editor de JSON en la Guía del usuario de IAM.

Prácticas recomendadas sobre las políticas

Identity-based las políticas determinan si alguien puede crear recursos de AWS Security Agent de su cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de

uso. Para obtener más información, consulte las políticas AWS administradas o las políticas administradas de AWS para las funciones laborales en la Guía del usuario de IAM.

- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Para obtener más información sobre cómo IAM aplicar permisos, consulte Políticas y permisos IAM en la Guía del usuario de IAM.
- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte Elementos de la política de IAM JSON: condición en la Guía del usuario de IAM.
- Úselo IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten al lenguaje de las políticas (JSON) y a las IAM mejores prácticas. IAM IAM Access Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarle a crear políticas seguras y funcionales. Para obtener más información, consulte la validación IAM Access Analyzer de políticas en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si se presenta una situación en la que se Usuarios de IAM requieren usuarios root en su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para obtener más información, consulte Configuración del acceso a la MFA-protected API en la Guía del usuario de IAM.

Uso de la consola de AWS Security Agent

Para acceder a la consola de AWS Security Agent, un director de IAM debe tener un conjunto mínimo de permisos. Estos permisos deben permitir al director enumerar y ver detalles sobre los recursos de AWS Security Agent de su propiedad Cuenta de AWS. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades principales que tengan esa política adjunta.

Para garantizar que sus directores de IAM puedan seguir utilizando la consola de AWS Security Agent, cree una política con su propio nombre exclusivo. Adjunte la política a las entidades

principales. Para obtener más información, consulte Agregar de permisos a un usuario en la Guía del usuario de IAM:

Para obtener información detallada sobre la política, consulte. the section called “Política gestionada por AWS: SecurityAgentWebAppAPIPolicy”

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Solución de problemas de identidad y acceso de AWS Security Agent

Utilice la siguiente información como ayuda para diagnosticar y solucionar problemas comunes que pueden surgir al trabajar con AWS Security Agent y IAM.

AccessDeniedException

Si recibe una `AccessDeniedException` al llamar a una operación de API de AWS, las credenciales principales de IAM que utiliza no tienen los permisos necesarios para realizar esa llamada.

```
An error occurred (AccessDeniedException) when calling the CreateEnvironment operation:
User: arn:aws:iam::111122223333:user/user_name is not authorized to perform:
securityagent:CreateEnvironment on resource:
 arn:aws:securityagent:region:111122223333:environment/my-env
```

En el mensaje de ejemplo anterior, el usuario no tiene permisos para llamar a la operación de la `CreateEnvironment` API de AWS Security Agent. Para proporcionar permisos de administrador de AWS Security Agent a un director de IAM, consultethe section called “Ejemplos de políticas basadas en la identidad de AWS Security Agent”.

Para obtener más información general sobre IAM, consulte Controlar el acceso a los recursos de AWS mediante políticas en la Guía del usuario de IAM.

Quiero permitir que personas ajenas a mi Cuenta de AWS para acceder a mis recursos de AWS Security Agent

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las

listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si AWS Security Agent admite estas funciones, consultethe section called “Cómo funciona AWS Security Agent con IAM”.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a uno Usuario de IAM en otro Cuenta de AWS que sea de su propiedad en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a sus recursos a terceros Cuentas de AWS, consulte Proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información acerca de cómo ofrecer acceso a la identidad federada, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer la diferencia entre el uso de funciones y políticas basadas en recursos para el acceso entre cuentas, consulte En qué se diferencian las IAM funciones de las políticas basadas en recursos en la Guía del usuario de IAM.

Respuesta a incidentes

AWS Security Agent es un servicio de pruebas de seguridad proactivas diseñado para identificar y prevenir las vulnerabilidades antes de que puedan explotarse. El servicio se centra en la validación preventiva de la seguridad mediante revisiones del diseño, análisis de código y pruebas de penetración, más que en la detección o respuesta reactivas a los incidentes.

Detección de incidentes

AWS Security Agent no ofrece capacidades de detección de incidentes. El servicio funciona como una herramienta de pruebas de seguridad proactivas que valida las aplicaciones para detectar vulnerabilidades durante el desarrollo y antes de su implementación. Para la supervisión de la seguridad en tiempo de ejecución y la detección de incidentes GuardDuty, utilice servicios como Amazon, AWS Security Hub o Amazon CloudWatch.

Alertas de incidentes

AWS Security Agent no genera alertas en tiempo real para incidentes de seguridad. El servicio proporciona los resultados de seguridad a través de la consola de AWS después de completar las revisiones de diseño, los análisis de código o las pruebas de penetración. Estos resultados representan posibles vulnerabilidades descubiertas durante las pruebas y no son incidentes de seguridad activos.

Remediación de incidentes

AWS Security Agent no proporciona una solución automática de incidentes. El servicio identifica las vulnerabilidades de seguridad y proporciona una guía de remediación, que incluye:

- Descripciones detalladas de las vulnerabilidades identificadas
- Rutas de explotación reproducibles para obtener resultados validados
- Correcciones de código específicas y orientación de implementación
- Análisis de impacto de los problemas descubiertos

Los equipos de desarrollo y seguridad utilizan esta guía para abordar manualmente las vulnerabilidades antes de que lleguen a los entornos de producción.

Apoyar las actividades de respuesta a incidentes

Si bien AWS Security Agent no está diseñado para responder a incidentes, los equipos de seguridad pueden utilizar el servicio para respaldar las actividades posteriores a los incidentes:

Validación de vulnerabilidades

: Tras un incidente de seguridad, utilice AWS Security Agent para comprobar si existen vulnerabilidades similares en otras aplicaciones o entornos.

Evaluación de la postura de seguridad

: Realice pruebas de penetración para validar las mejoras de seguridad implementadas como parte de la solución de incidentes.

Análisis de la causa raíz

: Utilice las funciones de revisión de la seguridad del código para identificar si pueden existir vulnerabilidades similares en otras bases de código.

Validación de conformidad para AWS Security Agent

Para saber si un servicio de AWS está dentro del ámbito de programas de conformidad específicos, consulte Servicios de AWS en Alcance por programa de conformidad y elija el programa de conformidad que le interese. Para obtener información general, consulte AWS Compliance Programs (Programas de conformidad de AWS).

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad de conformidad al utilizar los servicios de AWS viene determinada por la confidencialidad de sus datos, los objetivos de conformidad de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- Cumplimiento de seguridad y gobernanza: en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- Referencia de servicios válidos de HIPAA: muestra una lista con los servicios válidos de HIPAA. No todos los servicios de AWS cumplen con los requisitos de la HIPAA.
- Recursos de conformidad de AWS: es posible que este conjunto de guías y libros de ejercicios se apliquen a su sector y ubicación.
- Guías de conformidad para clientes de AWS: comprenda el modelo de responsabilidad compartida desde el punto de vista de la conformidad. Las guías resumen las prácticas recomendadas para proteger los servicios de AWS y mapean la guía con los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de recursos con reglas en la guía para desarrolladores de AWS: el servicio AWS Config evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este servicio de AWS proporciona una visión completa del estado de la seguridad en AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su conformidad con los estándares y las mejores prácticas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: este servicio de AWS detecta posibles amenazas para sus cuentas, cargas de trabajo, contenedores y datos de AWS mediante la supervisión de su entorno para detectar

actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por determinados marcos de conformidad.

- AWS Audit Manager: este servicio de AWS lo ayuda a auditar continuamente el uso de AWS a fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

Resiliencia en AWS Security Agent

> **Note**
>
> AWS Security Agent está disponible en las siguientes regiones: EE.UU. Este (Norte de Virginia) —`us-east-1`, EE.UU. Oeste (Oregón) —`us-west-2`, Asia Pacífico (Bombay) —`ap-south-1`, Asia Pacífico (Singapur) `ap-southeast-1` —, Asia Pacífico (Sídney) `ap-southeast-2` —, Asia Pacífico (Tokio) `ap-northeast-1` —, Europa (Fráncfort) `eu-central-1` —, Europa (Irlanda) `eu-west-1` — y Sudamérica (São Paulo) `sa-east-1` —. Utiliza la inferencia entre regiones. En Asia Pacífico (Bombay), Asia Pacífico (Singapur) y Sudamérica (São Paulo), AWS Security Agent utiliza la inferencia global entre regiones, que dirige las solicitudes de inferencia a cualquier región comercial de AWS. En todas las demás regiones, utiliza la inferencia geográfica entre regiones, que mantiene el procesamiento de datos dentro de límites geográficos específicos. AWS Security Agent es una herramienta que se utiliza durante el desarrollo de la aplicación y no debe implementarse como una infraestructura crítica o orientada al cliente.

La infraestructura global de AWS está conformada por regiones y zonas de disponibilidad de AWS. Las regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad y las regiones de AWS, consulte Infraestructura global de AWS.

Seguridad de la infraestructura en AWS Security Agent

Como servicio gestionado, AWS Security Agent está protegido por la seguridad de la red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y sobre cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS utilizando las prácticas recomendadas para la seguridad de la infraestructura, consulte Seguridad en el Well-Architected marco de AWS.

Aislamiento de red

AWS Security Agent es un servicio totalmente gestionado al que se accede a través de la consola de AWS y la aplicación web AWS Security Agent. El acceso al servicio se controla a través de AWS Identity and Access Management (IAM) o AWS IAM Identity Center, que se pueden integrar con su proveedor de identidad.

AWS Security Agent es compatible con los puntos de enlace de la VPC de la interfaz con la tecnología de AWS PrivateLink, lo que le permite acceder de forma privada a las API de servicio desde su VPC sin tener que atravesar la Internet pública. Para obtener más información, consulte the section called “Puntos de conexión de VPC de la interfaz”.

AWS Security Agent requiere acceso a Internet para realizar pruebas de penetración en las aplicaciones objetivo y para las operaciones del plano de control. El servicio utiliza la AWS-managed infraestructura para las pruebas y no aprovisiona instancias de EC2 ni otros recursos informáticos en su cuenta. Si configura el acceso a la VPC para las pruebas de penetración, Security Agent crea un ENI en la subred, pero este ENI no tiene una dirección IP pública. Para obtener más información, consulte the section called “Conectar el agente a los recursos de VPC privados”.

Multi-tenancy y aislamiento de recursos

AWS Security Agent es un servicio multiusuario. Las revisiones de seguridad, los hallazgos y los datos de los clientes se aíslan en cuentas individuales de AWS y se cifran en reposo. AWS aplica controles de aislamiento de infraestructura estándar para garantizar que las actividades de pruebas de seguridad de un cliente no afecten al rendimiento o la confidencialidad de otro cliente.

AWS Endpoints de VPC de interfaz y agente de seguridad (AWS PrivateLink)

Se puede utilizar AWS PrivateLink para crear una conexión privada entre la VPC y el AWS Security Agent. Puede acceder a Security Agent como si estuviera en su VPC, sin utilizar una puerta de

enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión Direct Connect. Las instancias de su VPC no necesitan direcciones IP públicas para acceder a Security Agent.

Esta conexión privada se establece mediante la creación de un punto de conexión de interfaz alimentado por AWS PrivateLink. Creamos una interfaz de red de punto de conexión en cada subred habilitada para el punto de conexión de interfaz. Se trata de interfaces de red administradas por el solicitante que sirven como punto de entrada para el tráfico destinado a Security Agent.

Para obtener más información, consulte Acceder a AWS los servicios AWS PrivateLink en la Guía. AWS PrivateLink

Consideraciones sobre Security Agent

Antes de configurar un punto final de interfaz para Security Agent, consulte las consideraciones de la AWS PrivateLink guía.

Security Agent permite realizar llamadas a todas sus acciones de API desde su VPC, incluidas las operaciones para administrar los espacios de los agentes, las pruebas de penetración y los hallazgos de seguridad.

Puede seleccionar IPv4, IPv6 o Dualstack al crear un punto final.

Security Agent admite políticas de puntos finales de VPC. De forma predeterminada, se permite el acceso total al Security Agent a través del punto final de la interfaz. Puede controlar el acceso adjuntando una política de punto final al punto final de la interfaz o asociando un grupo de seguridad a las interfaces de red del punto final.

Todas las llamadas de API a Security Agent se cifran mediante TLS 1.2 o superior, incluidas las llamadas realizadas a través de puntos de conexión de VPC. Para obtener más información sobre la protección de datos, consulte the section called “Protección de datos”. Las llamadas a la API de Security Agent se registran. AWS CloudTrail Para obtener más información, consulte the section called “Ejemplo: entradas del archivo de registro de AWS Security Agent”.

Cree un punto final de interfaz para Security Agent

Puede crear un punto final de interfaz para Security Agent mediante la consola de Amazon VPC o la interfaz de línea de AWS comandos (AWS CLI). Para obtener más información, consulte Crear un punto final de interfaz en la AWS PrivateLink guía.

Cree un punto final de interfaz para Security Agent con el siguiente nombre de servicio:

```
com.amazonaws.<region>.securityagent
```

Para crear el punto final de la interfaz mediante la AWS CLI, ejecute el siguiente comando. Sustituya la región, el ID de VPC, los ID de subred y el ID del grupo de seguridad por sus propios valores.

```
aws ec2 create-vpc-endpoint \
    --vpc-id vpc-1a2b3c4d \
    --vpc-endpoint-type Interface \
    --service-name com.amazonaws.<region>.securityagent \
    --subnet-ids subnet-1a2b3c4d subnet-5e6f7a8b \
    --security-group-ids sg-1a2b3c4d \
    --private-dns-enabled
```

Important

El DNS privado debe estar habilitado para el punto final de la interfaz. Security Agent requiere que utilice el nombre DNS regional predeterminado (por ejemplo`securityagent.us-east-1.api.aws`) para realizar solicitudes de API a través del punto final. No se admite llamar directamente a la URL de VPCE específica del punto final.

Para usar un DNS privado, debe establecer `enableDnsSupport` tanto los `enableDnsHostnames` atributos como `true` para la VPC. Para obtener más información, consulte Atributos de DNS para su VPC en la Guía del usuario de Amazon VPC.

Configure los grupos de seguridad para el punto final de la interfaz

Al crear un punto final de interfaz, puede asociar grupos de seguridad a las interfaces de red del punto final para controlar el tráfico hacia Security Agent. Cree un grupo de seguridad que permita el tráfico HTTPS entrante (puerto 443) desde los recursos de la VPC que necesitan comunicarse con Security Agent.

El grupo de seguridad debe incluir la siguiente regla de entrada:

- Tipo: HTTPS
- Protocolo: TCP
- Rango de puertos: 443

- Origen: el bloque CIDR de su VPC (por ejemplo`10.0.0.0/16`) o los ID de los grupos de seguridad de los recursos que necesitan acceso a Security Agent

Para obtener más información, consulte los grupos de seguridad en la AWS PrivateLink guía.

Creación de una política de puntos de conexión para el punto de conexión de interfaz

Una política de punto de conexión es un recurso de IAM que puede adjuntar a un punto de conexión de interfaz. La política de puntos finales predeterminada permite el acceso total al Security Agent a través del punto final de la interfaz. Para controlar el acceso permitido al Security Agent desde su VPC, adjunte una política de punto final personalizada al punto final de la interfaz.

Una política de punto de conexión especifica la siguiente información:

- Los principales que pueden realizar acciones (AWS cuentas, usuarios de IAM y funciones de IAM).
- Las acciones que se pueden realizar.
- El recurso en el que se pueden realizar las acciones.

Para obtener más información, consulte Controlar el acceso a los servicios mediante políticas de puntos finales en la Guía. AWS PrivateLink

Ejemplo: política de puntos finales de VPC para acciones de AWS Security Agent

El siguiente es un ejemplo de una política de puntos finales para AWS Security Agent. Cuando se adjunta a un punto final, esta política otorga acceso a las acciones enumeradas del AWS Security Agent a todos los responsables de todos los recursos.

```
{
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": [
            "securityagent:CreatePentest",
            "securityagent:ListPentests",
            "securityagent:BatchGetPentests",
            "securityagent:StartPentestExecution",
            "securityagent:StopPentestExecution",
            "securityagent:ListFindings",
```

```
            "securityagent:BatchGetFindings"
         ],
         "Resource": "*"
      }
   ]
}
```

Ejemplo: política de punto final de VPC que deniega todo acceso desde una cuenta específica AWS

La siguiente política de punto final de VPC deniega a la AWS cuenta `123456789012` todo acceso a los recursos que utilizan el punto final. La política permite todas las acciones de otras cuentas.

```
{
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": "securityagent:*",
         "Resource": "*"
      },
      {
         "Effect": "Deny",
         "Principal": {
            "AWS": "123456789012"
         },
         "Action": "securityagent:*",
         "Resource": "*"
      }
   ]
}
```

Resolución de problemas

La conexión se agota al llamar a la API de Security Agent

- Compruebe que el estado del punto final de la VPC sea: `available`

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-1a2b3c4d \
    --query "VpcEndpoints[].State"
```

- Confirme que el grupo de seguridad asociado al punto final permita el tráfico TCP entrante en el puerto 443 desde el CIDR de la VPC o el grupo de seguridad de origen.

- Compruebe que las tablas de enrutamiento de la VPC no enruten el tráfico del Security Agent a una puerta de enlace de Internet o a una puerta de enlace NAT en lugar de al punto final.

La resolución de DNS falla para **`securityagent.<region>.api.aws`**

- Compruebe que el DNS privado esté habilitado en el punto final:

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-1a2b3c4d \
    --query "VpcEndpoints[].PrivateDnsEnabled"
```

- Confirme que ambos `enableDnsSupport` `enableDnsHostnames` están configurados `true` en su VPC:

```
aws ec2 describe-vpc-attribute --vpc-id vpc-1a2b3c4d --attribute enableDnsSupport
aws ec2 describe-vpc-attribute --vpc-id vpc-1a2b3c4d --attribute enableDnsHostnames
```

`Access denied`errores al llamar a las API de Security Agent

- Compruebe la política de puntos finales de la VPC para asegurarse de que permite las acciones que intenta realizar.
- Compruebe que su política de identidad de IAM concede los permisos necesarios. `securityagent:`
- Si utilizas una política de puntos finales personalizada, confirma que tanto la política de puntos finales como la política de IAM permiten la solicitud.

Análisis de configuración y vulnerabilidad en AWS Security Agent

La configuración y los controles de TI son una responsabilidad compartida entre AWS y usted, nuestro cliente. Para obtener más información, consulte el modelo de responsabilidad compartida de AWS.

Cross-service prevención policial confusa

El problema del suplente confuso es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. Cross-service La suplantación de identidad puede producirse cuando un servicio (el

servicio de llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que le ayudan a proteger los datos de todos los servicios con directores de servicio a los que se les ha dado acceso a los recursos de su cuenta. Para obtener más información, consulte la Cross-service sección Prevención de errores administrativos en la Guía del usuario de AWS Identity and Access Management.

Prácticas recomendadas de seguridad para AWS Security Agent

AWS Security Agent proporciona una serie de características de seguridad que debe tener en cuenta a la hora de desarrollar e implementar sus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no constituyen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas.

Utilice entornos que no sean de producción para las pruebas de penetración

AWS Security Agent utiliza un conjunto completo de herramientas de pruebas de penetración de la distribución Kali Linux. Estas herramientas están diseñadas para identificar las vulnerabilidades de seguridad y pueden realizar acciones que modifiquen el estado de la aplicación, los datos o las configuraciones del sistema.

Práctica recomendada: Realice pruebas de penetración en entornos ajenos a la producción que reflejen su configuración de producción. Estos entornos de prueba deberían:

- No contener datos de clientes en tiempo real ni información de producción confidencial
- Manténgase aislado de los sistemas de producción
- Tienen configuraciones y controles de seguridad similares a los de producción
- No utilice credenciales para acceder a los sistemas de producción

Las pruebas en entornos de producción pueden resultar en:

- Modificación o eliminación de datos
- Interrupciones en el servicio o degradación del rendimiento
- Cambios de estado no deseados
- Activación de alertas de seguridad o procedimientos de respuesta a incidentes

Valide los hallazgos AI-generated de seguridad

AWS Security Agent realiza análisis de seguridad mediante agentes de IA. Debido a la naturaleza no determinista de los sistemas de IA, las pruebas de penetración pueden arrojar resultados variables según las distintas ejecuciones.

Práctica recomendada: valide las conclusiones de seguridad antes de tomar medidas correctivas:

- Revise los scripts de verificación generados por AWS Security Agent para cada hallazgo
- Ejecute los scripts de verificación en su entorno de prueba para confirmar la vulnerabilidad
- Considere la posibilidad de realizar varias pruebas de penetración para garantizar una cobertura completa
- Aplique un criterio de seguridad profesional para evaluar la gravedad y la explotabilidad de los hallazgos

Es posible que no todos los problemas identificados representen vulnerabilidades explotables en su contexto de implementación específico.

Revise y pruebe el código de corrección generado

AWS Security Agent puede generar correcciones de código y mejoras de seguridad para las vulnerabilidades identificadas. Estas AI-generated correcciones requieren una verificación antes de su implementación.

Práctica recomendada: revise todos los cambios de código generados:

- Examine las correcciones propuestas para comprobar si están completas y son correctas
- Pruebe las correcciones minuciosamente en entornos que no sean de producción
- Compruebe que las correcciones no introduzcan nuevas vulnerabilidades ni interrumpan la funcionalidad
- Utilice AWS Security Agent para volver a realizar la prueba después de aplicar las correcciones o ejecute los scripts de verificación proporcionados
- Siga los procesos de revisión y aprobación del código de su organización

Acceso al repositorio de códigos

AWS Security Agent puede proporcionar orientación de seguridad sobre los cambios de código mediante la integración de comentarios y revisiones de código. Para proteger la información de seguridad confidencial, esta funcionalidad funciona con restricciones específicas.

Limitación: la guía de seguridad del código está restringida únicamente a los repositorios privados. Esto garantiza que:

- Los hallazgos de seguridad permanecen confidenciales para su organización
- Las posibles vulnerabilidades no se divulgan públicamente antes de solucionarlas
- Las recomendaciones de corrección generadas no exponen los detalles de la explotación

AWS Security Agent no proporciona directrices de seguridad de código para los repositorios públicos. No comentará sobre los repositorios públicos ni los proyectos de código abierto en los que los hallazgos de seguridad puedan ser visibles públicamente.

Las pruebas de penetración de AWS Security Agent pueden revisar y corregir los repositorios públicos y privados que haya configurado para la prueba de registro. Si el repositorio es público, el código de corrección se proporcionará como un archivo diff descargable en lugar de como una solicitud de extracción de información.

URL accesibles

Las URL accesibles especifican puntos finales adicionales a los que el entorno de pruebas de penetración puede acceder durante las pruebas. Son necesarias cuando la aplicación depende de servicios externos, como proveedores de autenticación de terceros o CDN. Todas las dependencias de red necesarias para las pruebas deben especificarse como direcciones URL de destino o direcciones URL accesibles. La red bloquea el acceso a cualquier punto final no especificado.

Implicaciones de seguridad: AWS Security Agent no recibe instrucciones de realizar pruebas de seguridad en las URL accesibles. Al especificar las URL accesibles, indica confianza en estas dependencias. Los datos de las pruebas de penetración, incluidas las credenciales, pueden transmitirse a estos puntos finales de URL accesibles durante las pruebas.

Inferencia entre regiones

AWS Security Agent selecciona automáticamente la región óptima para procesar las solicitudes de inferencia. Esto maximiza los recursos informáticos disponibles, la disponibilidad de los modelos

y ofrece la mejor experiencia al cliente. Sus datos permanecen almacenados únicamente en la región en la que se originó la solicitud; sin embargo, es posible que las solicitudes de entrada y los resultados de salida se procesen fuera de esa región. Transmitimos todos los datos cifrados a través de la red de AWS.

AWS Security Agent utiliza dos tipos de inferencias entre regiones según la región:

- Inferencia geográfica entre regiones: mantiene el procesamiento de datos dentro de límites geográficos específicos (como EE. UU., UE, Australia o Japón) para la mayoría de las funciones. En el caso de la corrección del código, las solicitudes de Australia y Japón se tramitan en la Unión Europea. Se utiliza en EE.UU. Este (Norte de Virginia) —`us-east-1`, EE.UU. Oeste (Oregón) —`us-west-2`, Asia Pacífico (Sídney) —`ap-southeast-2`, Asia Pacífico (Tokio) —`ap-northeast-1`, Europa (Fráncfort) — `eu-central-1` y Europa (Irlanda) `eu-west-1` —.
- Inferencia global entre regiones: dirige las solicitudes de inferencia a cualquier región comercial de AWS, lo que optimiza los recursos disponibles y permite un mayor rendimiento del modelo. Utilizado en Asia Pacífico (Mumbai) —`ap-south-1`, Asia Pacífico (Singapur) `ap-southeast-1` — y Sudamérica (São Paulo) `sa-east-1` —.

En el caso de las regiones que utilizan la inferencia global entre regiones, las solicitudes de entrada y los resultados de salida se pueden procesar en cualquier región comercial de AWS. Todos los datos transmitidos durante las operaciones entre regiones permanecen en la red de AWS y no atraviesan la Internet pública. Encriptamos los datos en tránsito entre las regiones de AWS.

En la siguiente tabla se describe dónde se procesan las solicitudes de inferencia en función de la región en la que se originó la solicitud y de la función utilizada.

Origen de la solicitud	Todas las funciones excepto Code Remediation	Remediación de código
Estados Unidos — EE.UU. Este (Norte de Virginia) —`us-east-1` , EE.UU. Oeste (Oregón) — `us-west-2`	Estados Unidos	Estados Unidos
Unión Europea — Europa (Irlanda) `eu-west-1` —,	Unión Europea	Unión Europea

Origen de la solicitud	Todas las funciones excepto Code Remediation	Remediación de código
Europa (Fráncfort) — `eu-central-1`		
Australia — Asia Pacífico (Sídney) — `ap-southeast-2`	Australia	Unión Europea
Japón — Asia Pacífico (Tokio) — `ap-northeast-1`	Japón	Unión Europea
Sudamérica — Sudamérica (São Paulo) — `sa-east-1`	Cualquier región comercial de AWS	Cualquier región comercial de AWS
India — Asia Pacífico (Bombay) — `ap-south-1`	Cualquier región comercial de AWS	Cualquier región comercial de AWS
Sudeste Asiático — Asia-Pacífico (Singapur) — `ap-southeast-1`	Cualquier región comercial de AWS	Cualquier región comercial de AWS

Cross-Region La inferencia siempre está habilitada y no puede excluirse de ella. Cross-Region La inferencia no se ve afectada por las políticas de clientes de las Políticas de Control de Servicios (SCP) o de la Torre de Control de AWS, que restringen el contenido de los clientes a regiones específicas. Para obtener más información sobre cómo AWS Security Agent protege sus datos durante el procesamiento entre regiones, consulte Procesamiento de Cross-Region datos.

Migración de acciones y recursos de IAM

AWS Security Agent es un agente pionero que protege sus aplicaciones de forma proactiva durante todo el ciclo de vida del desarrollo en todos sus entornos. Si se incorporó a AWS Security Agent antes del 9 de febrero de 2026, se verá afectado por los cambios que se producirán el 9 de marzo de 2026 en sus recursos de instancias de agente actuales y en las acciones de IAM de AWS Security Agent. Como preparación para el lanzamiento del API/SDK soporte público, se cambiará el nombre del recurso Agent Instance por el de Agent Space y se cambiará el nombre de determinadas acciones de IAM. Estos cambios afectarán a cualquier función de IAM de aplicación o instancia de

agente que haya creado antes del 9 de marzo de 2026. Para evitar problemas de autenticación después del 9 de marzo de 2026, tendrá que seguir los pasos que se indican en Preparación para la migración.

> **Note**
>
> Si crea nuevas instancias de agente después del 9 de febrero de 2026, la nueva instancia de agente se creará como un espacio de agentes y no será necesario realizar ninguna migración.

Cambios planificados

AWS Security Agent está cambiando el nombre del recurso Agent Instance a Agent Space: `arn:aws:securityagent:us-east-1:{{accountId}}:agent-instance/*` renombrado `aarn:aws:securityagent:us-east-1:{{accountId}}:agent-space/*`. Además, se cambiará el nombre de las siguientes acciones de IAM:

- `securityagent:ListAgentInstances`Cambie el nombre de a `securityagent:ListAgentSpaces`
- `securityagent:ListControls`Cambie el nombre de a `securityagent:ListSecurityRequirements`
- `securityagent:BatchGetAgentInstances`Cambie el nombre de a `securityagent:BatchGetAgentSpaces`
- `securityagent:BatchGetSecurityTestContentMetadata`Cambie el nombre de a `securityagent:BatchGetPentestJobContentMetadata`
- `securityagent:BatchGetTasks`Cambie el nombre de a `securityagent:BatchGetPentestJobTasks`
- `securityagent:CreateDocumentReview`Cambie el nombre de a `securityagent:CreateDesignReview`
- `securityagent:GetDocumentReview`Cambie el nombre de a `securityagent:GetDesignReview`
- `securityagent:GetDocumentReviewArtifact`Cambie el nombre de a `securityagent:GetDesignReviewArtifact`
- `securityagent:ListDocumentReviews`Cambie el nombre de a `securityagent:ListDesignReviews`

- `securityagent:ListDocumentReviewComments`Cambie el nombre de a `securityagent:ListDesignReviewComments`
- `securityagent:ListTasks`Cambie el nombre de a `securityagent:ListPentestJobTasks`
- `securityagent:StartPentestExecution`Cambie el nombre de a `securityagent:StartPentestJob`
- `securityagent:StopPentestExecution`Cambie el nombre de a `securityagent:StopPentestJob`
- `securityagent:DeleteDocumentReview`Cambie el nombre de a `securityagent:DeleteDesignReview`

Preparándose para la migración

Para evitar problemas después del 9 de marzo de 2026 y seguir utilizando AWS Security Agent antes del 9 de marzo de 2026, tendrá que confiar en los recursos nuevos y antiguos y en las acciones de IAM de su IAM roles/policies hasta el 9 de marzo de 2026. Las siguientes instrucciones proporcionan una guía para migrar a los nuevos formatos de recursos y acciones:

1. Inicie sesión en su cuenta de AWS y vaya a la consola de AWS Security Agent.
2. En el panel de la izquierda, seleccione Configuración y elija el rol en Rol de servicio
3. En la consola de IAM del rol asociado, selecciona Añadir permisos y Adjuntar políticas
4. Seleccione AWSSecurityAgentWebAppPolicyy elija Agregar permisos
   a. Nota importante: compruebe que la ha seleccionado AWSSecurityAgentWebAppPolicycomo nueva política y no SecurityAgentWebAppAPIPolicy
5. Compruebe que su función de IAM ahora tenga ambas políticas de permisos AWSSecurityAgentWebAppPolicyy esté SecurityAgentWebAppAPIPolicyincluida en ellas
6. En la misma consola de roles de IAM, seleccione Relaciones de confianza y, a continuación, Editar política de confianza
7. Actualice su política de confianza al siguiente formato y sustituya {{AccountID}} por el ID de su cuenta de AWS

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

```
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{accountId}}"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:securityagent:us-east-1:{{accountId}}:application/*",
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-space/*",
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-instance/*"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:SetContext",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{accountId}}"
        },
        "ForAllValues:ArnEquals": {
          "sts:RequestContextProviders": "arn:aws:iam::aws:contextProvider/
IdentityCenter"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:securityagent:us-east-1:{{accountId}}:application/*",
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-space/*",
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-instance/*"
          ]
        }
      }
    }
  ]
```

```
}
```

8. Vuelva a la consola de AWS Security Agent. En el panel de la izquierda, selecciona Agent Spaces
9. Para cada espacio de agente que tenga habilitadas las pruebas de penetración, lleve a cabo los siguientes pasos
   a. Dirígete al espacio de agentes y selecciona Prueba de penetración
   b. En Acceso al servicio, elija el rol en el nombre del rol del servicio
   c. En la consola de IAM del rol asociado, seleccione Relaciones de confianza y, a continuación, Editar política de confianza
   d. Actualice su política de confianza al siguiente formato y sustituya {{AccountID}} por el ID de su cuenta de AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "securityagent.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{{accountId}}"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-space/*",
            "arn:aws:securityagent:us-east-1:{{accountId}}:agent-instance/*"
          ]
        }
      }
    }
  ]
}
```

Registro AWS La API de Security Agent se llama con AWS CloudTrail

AWS Security Agent está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en AWS Security Agent. CloudTrail captura todas las llamadas a la API de AWS Security Agent como eventos. Las llamadas capturadas incluyen llamadas desde la consola de AWS Security Agent y llamadas en código a las operaciones de la API de AWS Security Agent. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de AWS Security Agent. Si no configura un registro, podrá ver los eventos más recientes de la CloudTrail consola en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a AWS Security Agent, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

AWS Información sobre el agente de seguridad en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad en AWS Security Agent, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su AWS cuenta. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de los eventos de su AWS cuenta, incluidos los eventos de AWS Security Agent, cree un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando crea una ruta en la consola, la ruta se aplica a todas AWS las regiones. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de AWS Security Agent las registra CloudTrail. Por ejemplo, las llamadas a las `CreatePentest` `ListFindings` acciones y las llamadas generan entradas en los archivos de CloudTrail registro. `BatchGetPentestJobs`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o de AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Ejemplo: AWS Entradas del archivo de registro de Security Agent

Descripción AWS Entradas del archivo de registro de Security Agent

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `CreatePentest` acción:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2025-01-15T10:30:00Z",
```

```
    "eventSource": "securityagent.amazonaws.com",
    "eventName": "CreatePentest",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.12",
    "userAgent": "aws-cli/2.13.0",
    "requestParameters": {
        "pentestName": "WebApp-Security-Test",
        "targetUrl": "https://example.com",
        "testScope": "OWASP-Top-10"
    },
    "responseElements": {
        "pentestId": "pt-1234567890abcdef0",
        "pentestArn": "arn:aws:securityagent:us-east-1:123456789012:pentest/
pt-1234567890abcdef0"
    },
    "requestID": "a1b2c3d4-e5f6-7890-abcd-ef1234567890",
    "eventID": "12345678-1234-1234-1234-123456789012",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


Service Quotas

AWS Security Agent tiene cuotas que limitan la cantidad de recursos que puede crear y la velocidad a la que puede realizar operaciones. Las cuotas marcadas como ajustables se pueden aumentar enviando una solicitud a través de AWS Support. Para obtener más información, consulte Creación de casos de soporte y administración de casos.

Cuotas de operaciones

Las cuotas de operaciones limitan el uso mensual de las funciones de revisión y pruebas de seguridad para ayudar a gestionar la capacidad del servicio.

Recurso	Alcance	Cuota	Ajustable
Revisiones de diseño	Por mes, por cuenta y por región	200	Sí

Recurso	Alcance	Cuota	Ajustable
Reseñas de códigos PR	Por mes, por cuenta y por región	1 000	Sí

Cuotas de configuración

Las cuotas de configuración limitan la cantidad de recursos y ajustes que puede configurar en su entorno de AWS Security Agent.

Recurso	Alcance	Cuota	Ajustable
Espacios de agentes	Por cuenta por región	100	Sí
Integraciones	Por cuenta por región	20	No
Recursos integrados por integración	Por integración	50	No
Requisitos de seguridad personalizados	Por cuenta y por región	20	No
Proyectos Pentest	Por cuenta por región	1 000	Sí
Ejecuciones simultáneas de pentest	Por cuenta y por región	5	Sí
Proyectos de revisión de código	Por cuenta por región	1 000	Sí
Se ejecuta una revisión de código simultánea	Por cuenta y por región	5	Sí

Historial de revisión

En la siguiente tabla se describen algunas de las principales actualizaciones y nuevas funciones de la Guía del usuario de AWS Security Agents.

Cambio	Descripción	Fecha
Conexiones privadas (versión preliminar)	Se agregó documentación para las conexiones privadas.	16 de junio de 2026

	Esta nueva capacidad permite a AWS Security Agent conectarse a sistemas de control de código fuente que se ejecutan en redes privadas mediante Amazon VPC Lattice, sin exponer sus sistemas a la Internet pública.	
Modelado de amenazas (versión preliminar)	Se agregó documentación para el modelado de amenazas. Esta nueva capacidad crea un modelo de amenazas de su aplicación a partir de documentos de diseño (documentos de alcance), código fuente (fuentes) o ambos. Los documentos de alcance son documentos de diseño de funciones que definen el enfoque del análisis, mientras que el código fuente proporciona un contexto sobre el sistema actual. Si no proporciona los documentos de alcance, el agente genera un modelo de amenazas únicamente a partir del código fuente. Cada ejecución produce una descripción general del sistema y un conjunto de amenazas clasificadas por categoría de STRIDE con clasificaciones de gravedad y recomendaciones.	8 de junio de 2026

Revisión completa del código del repositorio (vista previa)	Se agregó documentación para una revisión completa del código del repositorio. Esta nueva capacidad realiza un análisis de seguridad contextual de toda la base de código y genera correcciones de código en función de los hallazgos.	12 de mayo de 2026
Se actualizó la disponibilidad regional para encontrar soluciones	Se ha actualizado la disponibilidad regional para realizar pruebas de penetración y encontrar soluciones en la aplicación web AWS Security Agent.	16 de abril de 2026
Se actualizó la disponibilidad regional para permitir la búsqueda de soluciones	Se ha actualizado la disponibilidad regional para permitir la búsqueda de soluciones en las pruebas de penetración en la consola de administración de AWS.	16 de abril de 2026
Admisión de claves administradas por el cliente	Se agregó documentación para el soporte de claves administradas por el cliente (CMK). Ahora puede especificar una clave KMS administrada por el cliente al crear espacios de agente e integraciones para cifrar sus datos con las claves que usted controle.	31 de marzo de 2026

AWS actualizaciones de políticas gestionadas	Se agregó una política AWSSecurityAgentWebAppPolicy administrada para los tipos nuevos TargetDomain y de DesignReviewFeedback recursos.	31 de marzo de 2026
AWS actualizaciones de políticas gestionadas	Se agregó una política AWSSecurityAgentWebAppPolicy administrada para el nuevo tipo de AgentSpace recurso y los cambios en el nombre de las acciones de IAM.	9 de febrero de 2026
AWS actualizaciones de políticas gestionadas	Se actualizó SecurityAgentWebAppAPIPolicy para permitir a los clientes eliminar las reseñas de diseño.	28 de enero de 2026
AWS actualizaciones de políticas gestionadas	Se actualizó SecurityAgentWebAppAPIPolicy para permitir a los clientes iniciar la corrección automática del código en caso de problemas de seguridad.	20 de enero de 2026
AWS actualizaciones de políticas gestionadas	Se actualizó SecurityAgentWebAppAPIPolicy para permitir a los clientes ver las imágenes en la consola.	5 de diciembre de 2025
Versión inicial de AWS Security Agents	Documentación inicial para el lanzamiento del servicio	2 de diciembre de 2025

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.