aws

Guía del usuario

Amazon Inspector

Amazon Inspector: Guía del usuario

Table of Contents

¿Qué es Amazon Inspector?

Amazon Inspector es un servicio de administración de vulnerabilidades que analiza de forma continua las cargas de trabajo de AWS en busca de vulnerabilidades de software y exposiciones de red no deseadas. Amazon Inspector detecta y analiza automáticamente las instancias de Amazon EC2, las imágenes de contenedores de Amazon Elastic Container Registry (Amazon ECR) y las funciones de AWS Lambda en ejecución en busca de vulnerabilidades de software conocidas y cualquier exposición de la red no deseada.

Amazon Inspector crea un hallazgo cuando detecta una vulnerabilidad de software o un problema de configuración de la red. En un hallazgo, se describe la vulnerabilidad, se identifica el recurso afectado, se califica la gravedad de la vulnerabilidad y se proporcionan directrices para su corrección. Puede analizar los hallazgos con la consola de Amazon Inspector o verlos y procesarlos a través de otros Servicios de AWS. Para obtener más información, consulte Descripción de los hallazgos de Amazon Inspector.

Temas

Características de Amazon Inspector

Administración centralizada de varias cuentas de Amazon Inspector

Si su entorno de AWS tiene varias cuentas, puede administrarlo de forma centralizada a través de una sola cuenta con AWS Organizations. De esta forma, puede designar una cuenta como cuenta de administrador delegado de Amazon Inspector.

Amazon Inspector se puede activar para toda la organización con un solo clic. También puede automatizar la activación del servicio para futuros miembros cuando se unan a la organización. Desde la cuenta de administrador delegado de Amazon Inspector, se administran los datos de los hallazgos, así como determinados parámetros para los miembros de la organización. Entre otras cosas, el administrador delegado puede ver detalles agregados de los hallazgos de todas las cuentas de miembros, activar o desactivar análisis de cuentas de miembros y revisar los recursos analizados dentro de la organización de AWS.

Análisis continuo del entorno en busca de vulnerabilidades y exposiciones de red

Con Amazon Inspector, no tendrá que programar o configurar manualmente análisis de evaluación. Amazon Inspector detecta automáticamente todos los recursos elegibles y empieza a analizarlos. Amazon Inspector sigue evaluando el entorno a lo largo del ciclo de vida de los recursos mediante el análisis continuo y automático de recursos en respuesta a los cambios que podrían haber introducido una nueva vulnerabilidad, como la instalación de un nuevo paquete en una instancia de EC2, la instalación de un parche y la publicación de una nueva lista de vulnerabilidades y riesgos comunes (CVE) que afectan al recurso. A diferencia de un software de análisis de seguridad tradicional, Amazon Inspector tiene un impacto mínimo en el rendimiento de la flota.

Cuando se detectan vulnerabilidades o rutas de red abiertas, Amazon Inspector genera un hallazgo para que lo investigue. El hallazgo incluye detalles exhaustivos sobre la vulnerabilidad y el recurso afectado, así como recomendaciones para corregir el problema. Siempre que se corrige un hallazgo correctamente, Amazon Inspector detecta automáticamente la corrección y cierra el hallazgo.

Evaluación de vulnerabilidades de forma precisa gracias a las puntuaciones de riesgo de Amazon Inspector

A medida que Amazon Inspector recopila información sobre el entorno mediante análisis, proporciona puntuaciones de gravedad adaptadas específicamente al entorno. Amazon Inspector examina las métricas de seguridad que componen la puntuación base de la Base de Datos Nacional de Vulnerabilidades (NVD) de los EE. UU. para una vulnerabilidad y las ajusta en función del entorno informático. Por ejemplo, el servicio puede reducir la puntuación de Amazon Inspector de un hallazgo para una instancia de Amazon EC2 si la vulnerabilidad se puede aprovechar a través de la red, pero no hay ninguna ruta de red abierta a la instancia que esté disponible en Internet. Esta puntuación se calcula con el formato CVSS y es una modificación de la puntuación base de Common Vulnerability Scoring System (CVSS) que proporciona la NVD.

Identificación de hallazgos de alto impacto con el panel de Amazon Inspector

El panel de Amazon Inspector ofrece una visualización de alto nivel de los hallazgos en todo el entorno. Desde el panel, puede acceder a los detalles pormenorizados de un hallazgo. El panel contiene información simplificada sobre la cobertura de los análisis en el entorno, los hallazgos más críticos y los recursos para los que se han generado más hallazgos. El panel de correcciones basadas en riesgos del panel de Amazon Inspector presenta los hallazgos que afectan al mayor número de instancias e imágenes. Este panel facilita la identificación de los hallazgos que afectan en mayor medida al entorno, la revisión de los detalles de los hallazgos y la consulta de las soluciones recomendadas.

Administración de los hallazgos con vistas personalizables

Además del panel, la consola de Amazon Inspector ofrece una vista de hallazgos. Esta página enumera todos los hallazgos del entorno y proporciona detalles de cada hallazgo. Puede ver los hallazgos agrupados por categoría o por tipo de vulnerabilidad. En cada vista, puede personalizar aún más los resultados mediante filtros. También puede utilizar filtros para crear reglas de supresión que oculten los resultados no deseados en las vistas.

Los filtros y las reglas de supresión le permiten generar informes sobre todos los hallazgos o sobre una selección personalizada de hallazgos. Los informes se pueden generar en formato CSV o JSON.

Supervisión y procesamiento de hallazgos con otros servicios y sistemas

Para facilitar la integración con otros servicios y sistemas, Amazon Inspector publica los hallazgos en Amazon EventBridge como eventos de resultado. EventBridge es un servicio de bus de eventos sin servidor que conecta los datos de los hallazgos con sus objetivos como, por ejemplo, funciones de AWS Lambda y temas de Amazon Simple Notification Service (Amazon SNS). Con EventBridge, puede supervisar y procesar los hallazgos casi en tiempo real como parte de sus flujos de trabajo de seguridad y cumplimiento.

Si ha activado AWS Security Hub, Amazon Inspector también publicará los hallazgos en Security Hub. Security Hub es un servicio que le proporciona una visión completa de su estado de seguridad en el entorno de AWS y le ayuda a verificar el entorno siguiendo los estándares y las prácticas recomendadas en el sector de la seguridad. Con Security Hub, puede supervisar y procesar los hallazgos de forma sencilla como parte de un análisis más completo del estado de seguridad de la organización en AWS.

Acceso a Amazon Inspector

Amazon Inspector está disponible en la mayoría de las Regiones de AWS. Para ver una lista de todas las regiones en las que Amazon Inspector está disponible en este momento, consulte Puntos de conexión y cuotas de Amazon Inspector en la Guía de referencia general de Amazon Web Services. Para obtener más información acerca de las Regiones de AWS, consulte Administración de Regiones de AWS en la Guía de referencia general de Amazon Web Services. En cada región, puede trabajar con Amazon Inspector de las siguientes formas.

Consola de administración de AWS

La AWS Management Console proporciona una interfaz de usuario basada en web que puede utilizar para crear y administrar recursos de AWS. Además, la consola de Amazon Inspector le otorga

acceso a su cuenta y recursos de Amazon Inspector. Desde la consola de Amazon Inspector puede llevar a cabo tareas de Amazon Inspector.

Herramientas de línea de comandos de AWS

Con las herramientas de línea de comandos de AWS, puede emitir comandos en la línea de comandos del sistema para llevar a cabo tareas de Amazon Inspector. Usar la línea de comandos puede ser más rápido y práctico que usar la consola. Las herramientas de línea de comandos también son útiles si desea crear scripts que realicen tareas.

AWS proporciona dos conjuntos de herramientas de línea de comandos: AWS Command Line Interface (AWS CLI) y la AWS Tools for PowerShell. Para obtener información sobre cómo instalar y utilizar la AWS CLI, consulte la Guía del usuario de la interfaz de línea de comandos de AWS. Para obtener información sobre cómo instalar y utilizar Tools for PowerShell, consulte la Guía del usuario de AWS Tools for PowerShell.

SDK de AWS

AWS ofrece SDK que se componen de bibliotecas y códigos de muestra para varios lenguajes de programación y plataformas, entre los que se incluyen Java, Go, Python, C++ y .NET. Los SDK proporcionan un acceso cómodo y programático a Amazon Inspector y otros Servicios de AWS. También permiten realizar tareas como firmar solicitudes criptográficamente, administrar errores y reintentar solicitudes automáticamente. Para obtener información sobre cómo instalar y utilizar los SDK de AWS, consulte Herramientas para compilar en AWS.

API de REST de Amazon Inspector

La API de REST de Amazon Inspector le proporciona un acceso completo y programático a su cuenta y recursos de Amazon Inspector. Con esta API, puede enviar solicitudes HTTPS directamente a Amazon Inspector. Sin embargo, a diferencia de las herramientas de línea de comandos y SDK de AWS, para utilizar esta API es necesario que la aplicación pueda realizar pequeñas tareas de nivel bajo, como generar para firmar una solicitud.

Introducción a Amazon Inspector

En este tutorial, encontrará una introducción práctica acerca de Amazon Inspector.

El paso 1 incluye la activación de los escaneos de Amazon Inspector para una cuenta independiente o como administrador delegado de Amazon Inspector AWS Organizations en un entorno de múltiples cuentas.

El paso 2 le ayuda a utilizar los hallazgos de Amazon Inspector en la consola.

> **Note**
>
> En este tutorial, completará las tareas en su versión actual. Región de AWS Para configurar Amazon Inspector en otras regiones, deberá completar estos pasos en cada una de las regiones.

Temas

Antes de empezar

Amazon Inspector es un servicio de administración de vulnerabilidades que analiza continuamente las instancias de Amazon EC2, las imágenes de los contenedores de Amazon ECR y las AWS Lambda funciones para detectar vulnerabilidades de software y exposiciones no intencionadas en la red.

Información importante antes de activar Amazon Inspector

- Amazon Inspector es un servicio regional y los datos se almacenan en el Región de AWS lugar donde se utiliza el servicio. Todos los procedimientos de configuración que complete en este tutorial deben repetirse en cada uno de los procedimientos de configuración Región de AWS que desee supervisar con Amazon Inspector.
- Amazon Inspector le ofrece la flexibilidad de activar la instancia de Amazon EC2, la imagen del contenedor de Amazon ECR y AWS Lambda el escaneo de funciones. Puede administrar los tipos

de análisis desde la página de administración de cuentas de la consola de Amazon Inspector o mediante las API de Amazon Inspector.

- Amazon Inspector puede proporcionar datos sobre vulnerabilidades y riesgos comunes (CVE) para sus instancias de EC2 solo si el agente de Amazon EC2 Systems Manager (SSM) está instalado y activado. Este agente viene preinstalado en muchas instancias de EC2, pero es posible que tenga que activarlo manualmente. Independientemente del estado del agente de SSM, se analizarán todas las instancias de EC2 en busca de problemas de exposición de red. Para obtener más información acerca de la configuración de análisis de Amazon EC2, consulte Análisis de instancias de Amazon EC2. Amazon ECR y el escaneo de AWS Lambda funciones no requieren el uso de un agente.
- Una identidad de usuario de IAM con permisos de administrador Cuenta de AWS puede habilitar Amazon Inspector. Con fines de protección de datos, le recomendamos que proteja sus credenciales y configure 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 administrar Amazon Inspector. Para obtener más información acerca de los permisos necesarios para habilitar Amazon Inspector, consulte AWS política gestionada: AmazonInspector2FullAccess.
- Al activar Amazon Inspector por primera vez en una región, se crea un rol vinculado a servicios a nivel mundial para la cuenta, denominado `AWSServiceRoleForAmazonInspector2`. Este rol incluye los permisos y las políticas de confianza que permiten a Amazon Inspector recopilar detalles de paquetes de software y analizar configuraciones de Amazon VPC para generar hallazgos de vulnerabilidades. Para obtener más información, consulte Uso de roles vinculados a servicios para Amazon Inspector. Para obtener más información acerca de los roles vinculados a servicios, consulte Uso de roles vinculados a servicios.

Paso 1: activación de Amazon Inspector

El primer paso antes de utilizar Amazon Inspector es activarlo para su Cuenta de AWS. Una vez haya activado cualquier tipo de análisis de Amazon Inspector, Amazon Inspector comenzará inmediatamente a descubrir y a analizar todos los recursos elegibles.

Si desea administrar Amazon Inspector para varias cuentas de su organización a través de una cuenta de administrador centralizada, deberá asignar un administrador delegado para Amazon Inspector. Elija una de las siguientes opciones para aprender a activar Amazon Inspector en su entorno.

Standalone account environment

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. Elija Comenzar.
3. Elija Activar Amazon Inspector.

Al activar Amazon Inspector en una cuenta independiente, todos los tipos de análisis se activan de forma predeterminada. Puede administrar los tipos de análisis activados desde la página de administración de cuentas de la consola de Amazon Inspector o mediante las API de Amazon Inspector. Una vez activado, Amazon Inspector detecta automáticamente todos los recursos elegibles y comienza a analizarlos. Revise la información sobre el tipo de análisis que se indica a continuación para conocer cuáles son los recursos elegibles de forma predeterminada:

Análisis de Amazon EC2

Para proporcionar datos sobre vulnerabilidades y exposiciones comunes (CVE) para su instancia EC2, Amazon Inspector requiere que el agente AWS Systems Manager (SSM) esté instalado y activado. Este agente viene preinstalado en muchas instancias de EC2, pero es posible que deba activarlo manualmente. Independientemente del estado del agente de SSM, se analizarán todas las instancias de EC2 en busca de problemas de exposición de red. Para obtener más información acerca de la configuración de análisis de Amazon EC2, consulte Análisis de instancias de Amazon EC2 con Amazon Inspector.

Análisis de Amazon ECR

Al activar el análisis de Amazon ECR, Amazon Inspector modifica todos los repositorios de contenedores de su registro privado que se hayan configurado con el valor Análisis básico proporcionado por Amazon ECR para que utilicen el valor Análisis mejorado y continuo. Si lo desea, también puede configurar este parámetro para que analice únicamente de forma automática o para que analice algunos repositorios según reglas de inclusión. Todas las imágenes insertadas en los últimos 30 días tienen programado el análisis por vigencia. Este parámetro de análisis de Amazon ECR puede modificarse en cualquier momento. Para obtener más información acerca de la configuración de análisis de Amazon ECR, consulte Análisis de imágenes de contenedores de Amazon ECR con Amazon Inspector.

AWS Lambda escaneo de funciones

Al activar el análisis de AWS Lambda funciones, Amazon Inspector descubre las funciones Lambda de su cuenta e inmediatamente comienza a analizarlas en busca de vulnerabilidades.

Amazon Inspector analiza las nuevas capas y funciones de Lambda cuando se implementan y vuelve a analizarlas cuando se actualizan o cuando se publican nuevas vulnerabilidades y riesgos comunes (CVE). Amazon Inspector ofrece dos niveles diferentes para el análisis de funciones de Lambda. De forma predeterminada, cuando activa Amazon Inspector por primera vez, se activa el análisis estándar de Lambda, por el que se analizan las dependencias de paquetes en las funciones. Asimismo, puede activar el análisis de código de Lambda para analizar el código de desarrollador de las funciones en busca de vulnerabilidades de código. Para obtener más información acerca de la configuración de análisis de funciones de Lambda, consulte AWS Lambda Funciones de escaneo con Amazon Inspector.

Multi-account environment

Important

Para completar estos pasos, debe estar en la misma organización que todas las cuentas que desee administrar y tener acceso a la cuenta de administración de AWS Organizations con el fin de delegar un administrador para Amazon Inspector en su organización. Es posible que se necesiten permisos adicionales para delegar un administrador. Para obtener más información, consulte Permisos necesarios para designar un administrador delegado.

Note

Si desea habilitar Amazon Inspector de forma programática para varias cuentas en varias regiones, puede utilizar un script de intérprete de comandos desarrollado por Amazon Inspector. Para obtener más información sobre el uso de este script, consulte inspector2 - on. enablement-with-cli GitHub

Designación de un administrador para Amazon Inspector

1. Inicie sesión en la cuenta de administración. AWS Organizations
2. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
3. En el panel Administrador delegado, introduzca el identificador de doce dígitos del Cuenta de AWS que desee designar como administrador delegado de Amazon Inspector para la

organización. A continuación, elija Delegar. En la ventana de confirmación, elija Delegar una vez más.

> **Note**
>
> Amazon Inspector se activa en su cuenta cuando delega un administrador.

Adición de cuentas de miembros

Como administrador delegado, puede activar el análisis para cualquier miembro asociado a la cuenta de administración de Organizations. Este flujo de trabajo activa todos los tipos de análisis para todas las cuentas de miembros. No obstante, los miembros también pueden activar Amazon Inspector en sus propias cuentas. El administrador delegado puede activar selectivamente los análisis para un servicio. Para obtener más información, consulte Administración de varias cuentas .

1. Inicie sesión en la cuenta del administrador delegado.
2. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
3. En el panel de navegación, elija Administración de cuentas. En la tabla Cuentas se muestran todas las cuentas de miembros asociadas a la cuenta de administración de Organizations.
4. En la página de administración de cuentas, puede seleccionar Activar el escaneo de todas las cuentas en la parte superior para activar las instancias de EC2, las imágenes de los contenedores de ECR y el escaneo de AWS Lambda funciones para todas las cuentas de su organización. También puede elegir las cuentas que desee añadir como miembros en la tabla Cuentas. A continuación, en el menú Activar, seleccione Todos los análisis.
5. (Opcional) Active la característica Activar Inspector automáticamente para las nuevas cuentas de miembros y seleccione los tipos de análisis que desee incluir para activar los análisis en todas las cuentas de miembro nuevas que se añadan a la organización.

Actualmente, Amazon Inspector ofrece escaneos para instancias EC2, imágenes de contenedores ECR y AWS Lambda funciones. Una vez activado, Amazon Inspector detecta automáticamente todos los recursos elegibles y comienza a analizarlos. Revise la información sobre el tipo de análisis que se indica a continuación para conocer cuáles son los recursos elegibles de forma predeterminada:

Análisis de Amazon EC2

Para proporcionar datos de vulnerabilidad de CVE para sus instancias EC2, Amazon Inspector requiere que el agente AWS Systems Manager (SSM) esté instalado y activado. Este agente viene preinstalado en muchas instancias de EC2, pero es posible que deba activarlo manualmente. Independientemente del estado del agente de SSM, se analizarán todas las instancias de EC2 en busca de problemas de exposición de red. Para obtener más información acerca de la configuración de análisis de Amazon EC2, consulte Análisis de instancias de Amazon EC2 con Amazon Inspector.

Análisis de Amazon ECR

Al activar el análisis de Amazon ECR, Amazon Inspector modifica todos los repositorios de contenedores de su registro privado que se hayan configurado con el valor Análisis básico proporcionado por Amazon ECR para que utilicen el valor Análisis mejorado y continuo. Si lo desea, también puede configurar este parámetro para que analice únicamente de forma automática o para que analice algunos repositorios según reglas de inclusión. Todas las imágenes insertadas en los últimos 30 días tienen programado el análisis por vigencia. El administrador delegado puede modificar este parámetro de análisis de Amazon ECR en cualquier momento. Para obtener más información acerca de la configuración de análisis de Amazon ECR, consulte Análisis de imágenes de contenedores de Amazon ECR con Amazon Inspector.

AWS Lambda escaneo de funciones

Al activar el análisis de AWS Lambda funciones, Amazon Inspector descubre las funciones Lambda de su cuenta e inmediatamente comienza a analizarlas en busca de vulnerabilidades. Amazon Inspector analiza las nuevas capas y funciones de Lambda cuando se implementan y vuelve a analizarlas cuando se actualizan o cuando se publican nuevas vulnerabilidades y riesgos comunes (CVE). Para obtener más información acerca de la configuración de análisis de funciones de Lambda, consulte AWS Lambda Funciones de escaneo con Amazon Inspector.

Paso 2: visualización de los hallazgos de Amazon Inspector

Puede ver los hallazgos de su entorno en la consola de Amazon Inspector o a través de la API. Todos los resultados también se envían a Amazon EventBridge y AWS Security Hub (si están activados). Además, los hallazgos relacionados con las imágenes de contenedores se envían a Amazon ECR.

La consola de Amazon Inspector ofrece varios formatos de visualización distintos para los hallazgos. El panel de Amazon Inspector proporciona información general de alto nivel sobre los riesgos que corre el entorno, mientras que la tabla Hallazgos le permite consultar los detalles de un hallazgo concreto.

En este paso, aprenderá a consultar los detalles de un hallazgo con la tabla Hallazgos y el panel correspondiente. Para obtener más información acerca del panel de Amazon Inspector, consulte Descripción del panel.

Visualización de detalles de los hallazgos de un entorno en la consola de Amazon Inspector

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. En el panel de navegación, seleccione Panel. Seleccione cualquiera de los enlaces del panel para acceder a una página de la consola de Amazon Inspector con más información sobre el elemento en cuestión.
3. En el panel de navegación, seleccione Hallazgos.
4. De forma predeterminada, verá la pestaña Todos los hallazgos, que muestra todos los hallazgos de la instancia EC2, la imagen del contenedor de ECR y las AWS Lambda funciones de su entorno.
5. En la lista Hallazgos, elija un nombre de hallazgo de la columna Título para abrir el panel de detalles correspondiente. Todos los hallazgos tienen la pestaña Detalles del hallazgo. Puede interactuar con la pestaña Detalles del hallazgo de las siguientes maneras:

   - Si desea obtener más información acerca de la vulnerabilidad, siga el enlace de la sección Detalles de la vulnerabilidad para abrir la documentación de dicha vulnerabilidad.
   - Si desea investigar más a fondo el recurso, siga el enlace ID de recurso de la sección Recurso afectado para abrir la consola de servicio del recurso afectado.

   Los hallazgos del tipo Vulnerabilidad de paquetes también incluyen la pestaña Puntuación de Inspector e inteligencia de vulnerabilidades, en la que se explica cómo se ha calculado la puntuación de Amazon Inspector de un hallazgo y se proporciona información sobre la lista de vulnerabilidades y riesgos comunes (CVE) asociada al hallazgo. Para obtener más información acerca de los tipos de hallazgo, consulte Tipos de hallazgos en Amazon Inspector.

Descripción del panel de Amazon Inspector

El panel de Amazon Inspector proporciona una instantánea de las estadísticas agregadas de los recursos de AWS en la región de AWS actual. Entre otras estadísticas, se incluyen métricas clave acerca de la cobertura de los recursos y las vulnerabilidades activas. En el panel también se muestran grupos de datos agregados de hallazgos para su cuenta, como instancias de Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Registry (Amazon ECR) y funciones de AWS Lambda con los hallazgos más críticos. Puede consultar los datos de soporte de los elementos del panel para llevar a cabo un análisis más profundo.

Si su cuenta es la del administrador delegado de Amazon Inspector de una organización, el panel incluirá la cobertura de la cuenta, las estadísticas agregadas y datos de los hallazgos de todas las cuentas de su organización, incluida su cuenta.

Visualización del panel

En el panel se ofrece una descripción general de la cobertura del entorno y de los hallazgos más críticos.

Visualización del panel

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2.
2. En el panel de navegación, elija Dashboard (Panel).
3. Puede interactuar con el panel de las siguientes formas:
   - El panel se actualiza automáticamente cada cinco minutos. Aun así, si desea actualizar los datos manualmente, seleccione el icono de actualización en la esquina superior derecha de la página.
   - Para ver los datos de soporte de un elemento del panel, elija un elemento.
   - Si administra varias cuentas de organizaciones de AWS como administrador delegado de Amazon Inspector, en el panel se mostrarán las estadísticas agregadas de las cuentas de miembros. Para filtrar el panel y consultar los datos solo para una cuenta determinada, introduzca el ID de cuenta en el cuadro Cuenta.

Descripción de los componentes del panel e interpretación de datos

Cada sección del panel de Amazon Inspector proporciona información acerca de las métricas clave o datos de los hallazgos activos para ayudarle a comprender la posición de vulnerabilidad de sus recursos de AWS en la Región de AWS actual.

Cobertura del entorno

La sección Cobertura del entorno proporciona estadísticas acerca de los recursos analizados por Amazon Inspector. En esta sección puede ver el recuento y el porcentaje de instancias de Amazon EC2, imágenes de Amazon ECR y funciones de AWS Lambda analizadas por Amazon Inspector. Si administra varias cuentas de AWS Organizations como administrador delegado de Amazon Inspector, también verá el número total de cuentas de la organización, el número de cuentas con Amazon Inspector activado y el porcentaje de cobertura resultante para la organización. Asimismo, esta sección le permite conocer los recursos que no están cubiertos por Amazon Inspector. Estos recursos pueden contener vulnerabilidades que podrían aprovecharse y poner en riesgo a la organización. Para obtener más información, consulte Evaluación de la cobertura de Amazon Inspector para el entorno de AWS.

Al elegir un grupo de cobertura, accederá a la página Administración de cuentas del grupo que haya seleccionado. En esta página se muestra detalles acerca de las cuentas, las instancias de Amazon EC2 y los repositorios de Amazon ECR que están cubiertos por Amazon Inspector.

Los grupos de cobertura disponibles son los siguientes:

- Cuenta
- Instancias
- Repositorios de contenedores
- Imágenes de contenedores
- Lambda

Hallazgos críticos

La sección Hallazgos críticos proporciona un recuento de las vulnerabilidades críticas del entorno y el total de hallazgos del entorno. En esta sección, los recuentos se muestran por recurso y tipo de evaluación. Para obtener más información acerca de los hallazgos críticos y sobre cómo Amazon Inspector calcula la gravedad, consulte Descripción de los hallazgos de Amazon Inspector.

Al elegir un grupo de hallazgos críticos, accederá a la página Todos los hallazgos, en la que se aplican automáticamente filtros para mostrar todos los hallazgos críticos que coincidan con el grupo que haya seleccionado.

Los grupos de hallazgos críticos disponibles son los siguientes:

- Hallazgos de imágenes de contenedores ECR
- Hallazgos de Amazon EC2
- Hallazgos de vulnerabilidades de accesibilidad de red
- Hallazgos de funciones de AWS Lambda

Correcciones basadas en riesgos

En la sección Correcciones basadas en riesgos se muestran los cinco paquetes de software con vulnerabilidades críticas que afectan a más recursos del entorno. Corregir estos paquetes reducirá significativamente el número de riesgos críticos en el entorno. Elija un nombre de paquete de software para ver los detalles de la vulnerabilidad asociada y los recursos afectados.

Cuentas con los hallazgos más críticos

En la sección Cuentas con los hallazgos más críticos se muestran las cinco cuentas de AWS del entorno con los hallazgos más críticos y el número total de hallazgos en esa cuenta. Esta sección solo se puede ver desde la cuenta del administrador delegado cuando Amazon Inspector está configurado para el análisis de varias cuentas con AWS Organizations. Esta vista ayuda a los administradores delegados a descubrir cuáles son las cuentas que corren el mayor riesgo dentro de la organización.

Elija ID de cuenta para obtener más información acerca de la cuenta de miembro afectada.

Repositorios de Amazon ECR con los hallazgos más críticos

En la sección Repositorios de Elastic Container Registry (ECR) con los hallazgos más críticos se muestran los cinco repositorios de Amazon ECR del entorno con los hallazgos de imágenes de contenedores más críticos. La vista muestra el nombre del repositorio, el identificador de cuenta de AWS, la fecha de creación del repositorio, el número de vulnerabilidades críticas y el número total de vulnerabilidades. Esta vista le ayuda a identificar los repositorios que corren el mayor riesgo.

Elija Nombre del repositorio para obtener más información acerca del repositorio afectado.

Imágenes de contenedores con los hallazgos más críticos

En la sección Imágenes de contenedores con los hallazgos más críticos se muestran las cinco imágenes de contenedores del entorno con los hallazgos más críticos. La vista muestra la fecha de etiquetado de la imagen, el nombre del repositorio, el resumen de imagen, el identificador de cuenta de AWS, el número de vulnerabilidades críticas y el número total de vulnerabilidades. Esta vista ayuda a los propietarios de aplicaciones a identificar las imágenes de contenedores que deberían recompilarse y volverse a iniciar.

Elija Imagen del contenedor para obtener más información acerca de la imagen de contenedor afectada.

Instancias con los hallazgos más críticos

En la sección Instancias con los hallazgos más críticos se muestran las cinco instancias de Amazon EC2 con los hallazgos más críticos. La vista muestra el identificador de la instancia, el identificador de cuenta de AWS, el identificador de la Imagen de máquina de Amazon (AMI), el número de vulnerabilidades críticas y el número total de vulnerabilidades. Esta vista ayuda a los propietarios de la infraestructura a identificar las instancias en las que es necesario aplicar revisiones.

Elija ID de la instancia para obtener más información acerca de la instancia de Amazon EC2 afectada.

Imágenes de máquina de Amazon (AMI) con los hallazgos más críticos

En la sección Imágenes de máquina de Amazon (AMI) con los hallazgos más críticos se muestran las cinco AMI del entorno con los hallazgos más críticos. La vista muestra el identificador de la AMI, el identificador de cuenta de AWS, el número de instancias de EC2 afectadas que se ejecutan en el entorno, la fecha de creación de la AMI, la plataforma del sistema operativo de la AMI, el número de vulnerabilidades críticas y el número total de vulnerabilidades. Esta vista ayuda a los propietarios de la infraestructura a identificar las AMI que pueden necesitar una recompilación.

Elija Instancias afectadas para obtener más información acerca de las instancias lanzadas desde la AMI afectada.

Funciones de AWS Lambda con los hallazgos más críticos

En la sección Funciones de AWS Lambda con los hallazgos más críticos se muestran las cinco funciones de Lambda del entorno con los hallazgos más críticos. La vista muestra el nombre de la función de Lambda, el identificador de cuenta de AWS, el entorno de ejecución,

el número de vulnerabilidades críticas, el número de vulnerabilidades altas y el número total de vulnerabilidades. Esta vista ayuda a los propietarios de la infraestructura a identificar las funciones de Lambda que deberían corregirse.

Elija Nombre de la función para obtener más información acerca de la función de AWS Lambda afectada.

Descripción de los hallazgos de Amazon Inspector

Un hallazgo es un informe detallado sobre una vulnerabilidad que afecta a uno de sus AWS recursos. Los resultados llevan el nombre de las vulnerabilidades detectadas y proporcionan clasificaciones de gravedad, información sobre los recursos afectados y detalles que describen cómo corregir las vulnerabilidades notificadas.

Amazon Inspector genera un hallazgo cada vez que detecta una vulnerabilidad en una instancia de Amazon EC2, una imagen de contenedor en un repositorio de Amazon ECR o una función. AWS Lambda Amazon Inspector analiza continuamente su entorno informático y almacena todos los hallazgos activos hasta que los corrija.

Cuando corriges un hallazgo, el hallazgo se cierra automáticamente y Amazon Inspector lo elimina al cabo de 7 días. Al eliminar un recurso, Amazon Inspector elimina cualquier hallazgo asociado al recurso después de 30 días.

Si inhabilitas Amazon Inspector, los resultados se eliminarán después de 24 horas. Si AWS suspende tu cuenta, los resultados se eliminarán después de 90 días.

Los hallazgos se clasifican en uno de los siguientes estados:

Activo

: Amazon Inspector identifica como Activos los hallazgos que no se han corregido.

Suprimido

: Amazon Inspector identifica los hallazgos que están sujetos a una o más normas de supresión como suprimidos. Puede encontrar los hallazgos suprimidos en la lista de hallazgos suprimidos. Para obtener más información, consulte Supresión de hallazgos de Amazon Inspector mediante reglas de supresión.

Cerrado

: Tras corregir una vulnerabilidad, Amazon Inspector la detecta automáticamente y cambia el estado del hallazgo a Cerrado. Los hallazgos cerrados se eliminan después de 7 días.

Temas

- Localización y visualización de los hallazgos de Amazon Inspector
- Detalles de los hallazgos de Amazon Inspector
- Puntuación de Amazon Inspector e inteligencia de vulnerabilidades
- Niveles de gravedad de los hallazgos de Amazon Inspector

Tipos de hallazgos en Amazon Inspector

Amazon Inspector genera hallazgos a partir de instancias de Amazon Elastic Compute Cloud (Amazon EC2), imágenes de contenedores almacenadas en repositorios de Amazon Elastic Container Registry (Amazon ECR) y funciones de AWS Lambda. Amazon Inspector puede generar los siguientes tipos de hallazgos.

Vulnerabilidad de paquetes

Los hallazgos de vulnerabilidades de paquetes identifican los paquetes de software de su entorno de AWS expuestos a vulnerabilidades y riesgos comunes (CVE). Los atacantes pueden aprovechar las vulnerabilidades no parcheadas y poner en riesgo la confidencialidad, integridad o disponibilidad de los datos, así como acceder a otros sistemas. El sistema de CVE sirve como método de referencia para las vulnerabilidades y exposiciones de seguridad de la información conocidas. Para obtener más información, visite https://www.cve.org/.

Los avisos de seguridad de los proveedores agregan las CVE detectadas en Linux a Amazon Inspector en un plazo de 24 horas tras su publicación. Microsoft agrega las CVE detectadas en Windows en un plazo de 48 horas tras su publicación. Utilice la Búsqueda en la base de datos de vulnerabilidades de Amazon Inspector para comprobar si se admite una CVE detectada.

Amazon Inspector puede generar hallazgos de vulnerabilidades de paquetes sobre instancias de EC2, imágenes de contenedores de ECR y funciones de Lambda. Los hallazgos de vulnerabilidades de paquetes ofrecen más detalles únicos acerca de este tipo de hallazgo: la puntuación de Inspector e inteligencia de vulnerabilidades.

Vulnerabilidad de código

Los hallazgos de vulnerabilidades de código identifican las líneas de código que pueden aprovechar posibles atacantes. Entre las vulnerabilidades de código se incluyen fallos de inyección, fugas de datos, errores de criptografía débil o una falta de cifrado en el código.

Amazon Inspector evalúa el código de la aplicación de la función de Lambda mediante razonamiento automatizado y machine learning de conformidad con los estándares generales de seguridad. Identifica las infracciones de políticas y las vulnerabilidades en función de detectores internos desarrollados en colaboración con Amazon CodeGuru. Para consultar una lista de posibles detecciones, vaya a la biblioteca de detectores de CodeGuru.

> **Important**
>
> El análisis de código de Amazon Inspector captura fragmentos de código para resaltar las vulnerabilidades detectadas. Estos fragmentos pueden contener credenciales codificadas u otros tipos de información confidencial en formato de texto no cifrado.

Amazon Inspector puede generar hallazgos del tipo Vulnerabilidad de código para las funciones de Lambda si el Análisis de código de Lambda con Amazon Inspector está activado.

Los fragmentos de código que se detectan junto a un hallazgo de vulnerabilidad de código se almacenan en el servicio CodeGuru. De forma predeterminada, se utiliza una clave propiedad de AWS controlada por CodeGuru para cifrar el código. No obstante, puede utilizar su propia clave administrada por el cliente para cifrarlo a través de la API de Amazon Inspector. Para obtener más información, consulte Cifrado de código en reposo en los hallazgos .

Accesibilidad de red

Los hallazgos de accesibilidad de red indican que hay rutas de red abiertas a las instancias de Amazon EC2 de su entorno. Estos hallazgos aparecen cuando se puede acceder a los puertos TCP y UDP desde las periferias de VPC mediante una puerta de enlace de Internet (incluidas las instancias situadas detrás de equilibradores de carga de aplicaciones o equilibradores de carga clásicos), una conexión de emparejamiento de VPC o una VPN a través de una puerta de enlace virtual. En estos hallazgos se destacan las configuraciones de red que podrían ser demasiado permisivas, entre las que se incluyen grupos de seguridad mal administrados, listas de control de acceso o puertas de enlace de Internet, que podrían permitir un acceso potencialmente malicioso.

Amazon Inspector solo genera hallazgos de accesibilidad de red para instancias de Amazon EC2. Amazon Inspector lleva a cabo un análisis de accesibilidad de red cada 24 horas.

Amazon Inspector evalúa las siguientes configuraciones cuando se analizan las rutas de red:

- Instancias de Amazon EC2

- Funciones de AWS Lambda
- Equilibrador de carga de aplicación
- Direct Connect
- Elastic Load Balancers
- Interfaces de redes elásticas
- Puertas de enlace de Internet
- Listas de control de acceso a la red
- Tablas de enrutamiento
- Grupos de seguridad
- Subredes
- Nubes privadas virtuales
- Puertas de enlace privadas virtuales
- Puntos de conexión de VPC
- Puntos de conexión de puertas de enlace de VPC
- Interconexiones de VPC
- Conexiones de VPN

Localización y visualización de los hallazgos de Amazon Inspector

Los procedimientos de esta sección describen cómo localizar y ver los hallazgos en Amazon Inspector a través de la consola y la API de Amazon Inspector. Los detalles de búsqueda varían según el tipo de búsqueda, el tipo de vulnerabilidad y los recursos afectados. Para obtener más información, consulte Detalles de los hallazgos de Amazon Inspector.

Console

Visualización de los resultados en la consola

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. En el panel de navegación, seleccione Findings. Se le dirigirá a una pantalla de hallazgos en la que podrá ver todos sus hallazgos. En la tabla de hallazgos, puede elegir un hallazgo seleccionando el nombre del hallazgo en la columna Título.

3. (Opcional) También puede ver los hallazgos agrupados por categoría. En el panel de navegación, elija Hallazgos y, a continuación, elija una de las siguientes categorías:

   - Por vulnerabilidad
   - Por instancia

     > **Note**
     >
     > Los resultados agrupados por instancia no incluyen información sobre la disponibilidad de la red.

   - Por imagen de contenedor
   - Por repositorio de contenedores
   - Por función Lambda

API

Use la operación de la API de ListFindings. En la solicitud, puede especificar `filterCriteria` para que se obtengan resultados específicos.

Detalles de los hallazgos de Amazon Inspector

En la consola de Amazon Inspector, puede consultar los detalles de cada hallazgo. Los detalles de los hallazgos varían según el tipo de hallazgo.

Consulta de los detalles de un hallazgo

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. Seleccione la región en la que desea ver los resultados.
3. En el panel de navegación, elija Hallazgos para ver la lista de hallazgos.
4. (Opcional) Utilice la barra de filtros para seleccionar un hallazgo específico. Para obtener más información, consulte Filtrado de hallazgos de Amazon Inspector.
5. Elija un resultado para abrir el panel de detalles correspondiente.

La pestaña Detalles del resultado contiene las características identificativas básicas del resultado. Esto incluye el título del resultado, una descripción breve de la vulnerabilidad identificada,

sugerencias para corregirla y una puntuación de gravedad. Para obtener más información acerca de las puntuaciones, consulte Niveles de gravedad de los hallazgos de Amazon Inspector.

Los detalles disponibles acerca de un hallazgo varían según el tipo de hallazgo y el recurso afectado.

Todos los hallazgos contienen el número de Cuenta de AWS identificación por el que se identificó el hallazgo, la gravedad, el tipo de hallazgo, la fecha en que se creó el hallazgo y una sección sobre el recurso afectado con detalles sobre ese recurso.

El tipo de hallazgo determina la información de inteligencia sobre correcciones y vulnerabilidades disponible para ese hallazgo. Según el tipo de hallazgo, hay diferentes detalles disponibles.

Vulnerabilidad de paquetes

Los hallazgos de vulnerabilidad de paquetes están disponibles para instancias de EC2, imágenes de contenedores de ECR y funciones de Lambda. Consulte Vulnerabilidad de paquetes para obtener más información.

Los hallazgos de vulnerabilidad de paquetes también incluyen la Puntuación de Amazon Inspector e inteligencia de vulnerabilidades.

Este tipo de hallazgo incluye los siguientes detalles:

- Corrección disponible: indica si la vulnerabilidad está corregida en una versión más reciente de los paquetes afectados. Puede tener uno de los siguientes valores:
  - `YES`, lo que significa que todos los paquetes afectados tienen una versión corregida.
  - `NO`, lo que significa que ningún paquete afectado tiene una versión corregida.
  - `PARTIAL`, lo que significa que uno o más de los paquetes afectados (pero no todos) tienen una versión corregida.
- Explotación disponible: indica que la vulnerabilidad tiene una explotación conocida.
  - `YES`, lo que significa que la vulnerabilidad descubierta en el entorno tiene una explotación conocida. Amazon Inspector no puede consultar el uso de explotaciones en un entorno.
  - `NO`, lo que significa que esta vulnerabilidad no tiene ninguna explotación conocida.
- Paquetes afectados: muestra todos los paquetes identificados como vulnerables en el hallazgo y los detalles de cada paquete.
- Ruta de archivo: el identificador del volumen de EBS y el número de partición asociados a un resultado. Este campo está presente en los resultados de las instancias de EC2 analizadas con Análisis sin agente.

- Versión instalada/Versión corregida: indica el número de versión del paquete instalado actualmente para el que se ha detectado una vulnerabilidad. Compare el número de la versión instalada con el valor que aparece después de la barra diagonal (/). El segundo valor es el número de versión del paquete en el que se corrige la vulnerabilidad detectada, tal como se indica en la lista de vulnerabilidades y riesgos comunes (CVE) o el aviso relacionado con el hallazgo. Si la vulnerabilidad se ha corregido en varias versiones, en este campo se muestra la versión más reciente que incluye la corrección. Si no hay una solución disponible, el valor que se muestra es `None available`.

  > **Note**
  >
  > Si se detectó un hallazgo antes de que Amazon Inspector empezará a incluir este campo en los hallazgos, el valor de este campo estará vacío. No obstante, es posible que haya disponible una corrección.

- Administrador de paquetes: el administrador de paquetes utilizado para configurar este paquete.
- Corrección: si hay una corrección disponible en un paquete actualizado o una biblioteca de programación, en esta sección se incluyen los comandos que puede ejecutar para llevar a cabo la actualización. Puede copiar el comando proporcionado y ejecutarlo en el entorno.

  > **Note**
  >
  > Los comandos de corrección provienen de las fuentes de datos de los proveedores y pueden variar en función de la configuración del sistema. Consulte las referencias sobre hallazgos o la documentación del sistema operativo para obtener instrucciones más específicas.

- Detalles de vulnerabilidades: proporciona un enlace a la fuente preferida de Amazon Inspector para la CVE identificada en el hallazgo, como la Base de Datos Nacional de Vulnerabilidades (NVD) de los EE. UU., Red Hat u otro proveedor de sistemas operativos. Además, incluye las puntuaciones de gravedad del hallazgo. Para obtener más información acerca de las puntuaciones de gravedad, consulte Niveles de gravedad de los hallazgos de Amazon Inspector. Se incluyen las siguientes puntuaciones, incluidos los vectores de puntuación de cada una:
  - Puntuación de EPSS
  - Puntuación de Inspector

- CVSS 3.1 de CVE de Amazon
- CVSS 3.1 de NVD
- CVSS 2.0 de NVD (si procede, para CVE antiguas)

- Vulnerabilidades relacionadas: especifica otras vulnerabilidades relacionadas con el hallazgo. Por lo general, se trata de otras CVE que afectan a la misma versión del paquete o de otras CVE del mismo grupo que la CVE del hallazgo, según lo determinado por el proveedor.

Vulnerabilidad de código

Los hallazgos de vulnerabilidades del código solo están disponibles para las funciones de Lambda. Consulte Vulnerabilidad de código para obtener más información. Este tipo de hallazgo incluye los siguientes detalles:

- Corrección disponible: en el caso de las vulnerabilidades del código, este valor siempre es `YES`.
- Nombre del detector: el nombre del CodeGuru detector utilizado para detectar la vulnerabilidad del código. Para obtener una lista de posibles detecciones, consulte la biblioteca de CodeGuru detectores.
- Etiquetas de detector: las CodeGuru etiquetas asociadas al detector CodeGuru utilizan etiquetas para categorizar las detecciones.
- CWE relevante: los ID de la enumeración de puntos débiles comunes (CWE) asociados con la vulnerabilidad de código.
- Ruta de archivo: la ubicación del archivo de la vulnerabilidad de código.
- Ubicación de la vulnerabilidad: en el caso de las vulnerabilidades del código en las que se analiza el código de Lambda, en este campo se muestran las líneas exactas de código en las que Amazon Inspector ha encontrado la vulnerabilidad.
- Solución sugerida: sugiere cómo se puede editar el código para corregir el hallazgo.

Accesibilidad de red

Los resultados de accesibilidad de la red solo están disponibles para las instancias de EC2. Consulte Accesibilidad de red para obtener más información. Este tipo de hallazgo incluye los siguientes detalles:

- Rango de puertos abierto: indica el rango de puertos a través del cual se ha podido acceder a la instancia de EC2.
- Rutas de red abierta: muestra la ruta de acceso abierta a la instancia de EC2. Seleccione un elemento de la ruta para obtener más información.
- Corrección: recomienda un método para cerrar la ruta de red abierta.

Puntuación de Amazon Inspector e inteligencia de vulnerabilidades

En la consola de Amazon Inspector, al seleccionar un resultado, puede ver la pestaña Puntuación de Inspector e inteligencia de vulnerabilidades, en la que se muestran los detalles de puntuación de un resultado de vulnerabilidad de paquetes, así como detalles de la inteligencia de vulnerabilidades. Estos detalles solo están disponibles para los hallazgos de Vulnerabilidad de paquetes.

Puntuación de Amazon Inspector

La puntuación de Amazon Inspector es una puntuación contextualizada que Amazon Inspector crea para cada hallazgo de una instancia de EC2. Para calcular esta puntuación, se correlaciona la información de la puntuación base CVSS v3.1 con información recopilada del entorno informático durante los análisis, que puede incluir resultados de accesibilidad de red y datos de explotabilidad. Por ejemplo, la puntuación de Amazon Inspector de un hallazgo puede ser inferior a la puntuación base si la vulnerabilidad se puede explotar a través de la red, pero Amazon Inspector determina que no hay ninguna ruta de red abierta a la instancia vulnerable que esté disponible en Internet.

La puntuación base de un hallazgo es la puntuación base CVSS v3.1 proporcionada por el proveedor. Se admiten las puntuaciones base de proveedores como RHEL, Debian o Amazon. Si se utilizan otros proveedores o si el proveedor no ha proporcionado una puntuación, Amazon Inspector utilizará la puntuación base de la Base de Datos Nacional de Vulnerabilidades (NVD) de los EE. UU. Amazon Inspector utiliza la calculadora de Common Vulnerability Scoring System, versión 3.1, para obtener una puntuación. Puede ver el origen de la puntuación base de un resultado en los detalles de este en Detalles de vulnerabilidades, por ejemplo en Fuente de vulnerabilidad (o en packageVulnerabilityDetails.source en el archivo JSON del resultado).

> **Note**
>
> La puntuación de Amazon Inspector no está disponible para las instancias de Linux que ejecutan Ubuntu. Esto se debe a que Ubuntu define su propia gravedad para las vulnerabilidades, que puede diferir de la gravedad que se asigna en la CVE asignada.

Detalles de la puntuación de Amazon Inspector

Al abrir la página de detalles de un resultado, puede seleccionar la pestaña Puntuación de Inspector e inteligencia de vulnerabilidades. Este panel muestra la diferencia entre la puntuación base y la puntuación de Inspector. En esta sección se explica cómo Amazon Inspector asignó la clasificación

de gravedad en función de una combinación de la puntuación de Amazon Inspector y la puntuación del proveedor para el paquete de software. Si las puntuaciones difieren, en este panel se explica por qué.

En la sección Métricas de puntuación CVSS, puede consultar una tabla de comparaciones entre las métricas de puntuación base CVSS y la puntuación de Inspector. Las métricas comparadas son las métricas base definidas en el documento de especificaciones de CVSS, mantenido por first.org. A continuación se proporciona un resumen de cada métrica base:

Vector de ataque

Se trata del contexto en el que se puede aprovechar una vulnerabilidad. En el caso de los hallazgos de Amazon Inspector, puede ser Red, Red adyacente o Local.

Complejidad del ataque

Describe el nivel de dificultad al que se enfrentará un atacante al aprovechar la vulnerabilidad. Si se asigna una puntuación baja, el atacante tendrá que cumplir pocas condiciones adicionales (o ninguna) para aprovechar la vulnerabilidad. En cambio, si la puntuación es alta, el atacante necesitará invertir una cantidad considerable de esfuerzo para llevar a cabo un ataque exitoso con esta vulnerabilidad.

Privilegios necesarios

Describe el nivel de privilegios que necesitará un atacante para aprovechar una vulnerabilidad.

Interacción del usuario

Esta métrica indica si un ataque exitoso que aproveche esta vulnerabilidad requiere interacción de otra persona que no sea el atacante.

Scope (Ámbito)

Indica si una vulnerabilidad en un componente vulnerable afecta a los recursos de los componentes que están fuera del ámbito de seguridad del componente vulnerable. Si el valor es Sin cambios, el recurso vulnerable y el recurso afectado son el mismo. Si el valor es Cambiado, se puede aprovechar el componente vulnerable para afectar a los recursos administrados por diferentes autoridades de seguridad.

Confidencialidad

Mide el nivel de impacto en la confidencialidad de los datos de un recurso cuando se aprovecha la vulnerabilidad. El valor oscila entre Ninguna, según el cual no se pierde confidencialidad,

y Alta, según el cual se divulga toda la información de un recurso o se puede divulgar datos confidenciales como contraseñas o claves de cifrado.

Integridad

Mide el nivel de impacto en la integridad de los datos del recurso afectado cuando se aprovecha la vulnerabilidad. La integridad corre peligro cuando el atacante modifica los archivos de los recursos afectados. La puntuación oscila entre Ninguna, según la cual el atacante no puede modificar información a través de esta vulnerabilidad, y Alta, según la cual, si se aprovecha la vulnerabilidad, el atacante podría modificar cualquier archivo o la posible modificación de archivos daría lugar a graves consecuencias.

Disponibilidad.

Mide el nivel de impacto en la disponibilidad del recurso afectado cuando se aprovecha la vulnerabilidad. La puntuación oscila entre Ninguna, según la cual la vulnerabilidad no afecta en absoluto a la disponibilidad, y Alta, según la cual, si se aprovecha la vulnerabilidad, el atacante puede denegar completamente la disponibilidad del recurso o provocar la falta de disponibilidad de un servicio.

Inteligencia de vulnerabilidades

En esta sección se resume la inteligencia disponible sobre las CVE de Amazon y otras fuentes de inteligencia sobre seguridad estándar en el sector, como Recorded Future y Cybersecurity and Infrastructure Security Agency (CISA).

> **Note**
>
> La inteligencia de CISA, Amazon o Recorded Future no estará disponible para todas las CVE.

Puede consultar los detalles de la inteligencia de vulnerabilidades en la consola o con la API BatchGetFindingDetails. En la consola están disponibles las siguientes métricas:

ATT y CK

En esta sección se muestran las tácticas, técnicas y procedimientos (TTP) de MITRE asociados a la CVE. Se muestran las TTP asociadas y, si hay más de dos TTP aplicables, puede seleccionar

el enlace para ver una lista completa. Al seleccionar una táctica o técnica, se abre información al respecto en el sitio web de MITRE.

CISA

Esta sección cubre las fechas relevantes asociadas a la vulnerabilidad. La fecha en la que Cybersecurity and Infrastructure Security Agency (CISA) añadió la vulnerabilidad al catálogo de vulnerabilidades aprovechadas y conocidas, según pruebas de una explotación activa, y la fecha límite en la que CISA espera que se hayan arreglado los sistemas. Esta información proviene de CISA.

Malware conocido

En esta sección se enumeran los kits y las herramientas conocidos que aprovechan esta vulnerabilidad.

Evidencia

En esta sección se resumen los eventos de seguridad más críticos relacionados con esta vulnerabilidad. Si hay más de tres eventos con el mismo nivel de gravedad, se muestran los tres eventos más recientes.

Última vez informado

En esta sección se muestra la fecha de la última explotación pública conocida de esta vulnerabilidad.

Niveles de gravedad de los hallazgos de Amazon Inspector

Cuando Amazon Inspector genera un hallazgo de vulnerabilidad, asigna automáticamente una gravedad al hallazgo. La gravedad de un hallazgo indica las características principales del hallazgo para ayudarle a evaluar y priorizar los hallazgos. La gravedad de un hallazgo no refleja de ningún modo la importancia o la gravedad que pueda tener un recurso afectado para su organización.

La clasificación de gravedad de un hallazgo se basa en una puntuación numérica que se corresponde con uno de los siguientes niveles de gravedad: informativa, baja, media, alta o crítico.

El método por el que Amazon Inspector determina la gravedad varía según el tipo de hallazgo. Consulte las siguientes secciones para obtener más información sobre cómo Amazon Inspector determina la clasificación de gravedad de cada tipo de hallazgo.

Gravedad de una vulnerabilidad de paquetes de software

Amazon Inspector utiliza la puntuación NVD/CVSS como base para la puntuación de gravedad de las vulnerabilidades de paquetes de software. La puntuación NVD/CVSS es la puntuación de gravedad de la vulnerabilidad publicada por NVD y definida por CVSS. Combina varias métricas de seguridad como la complejidad del ataque, la madurez del código de vulneración y los privilegios necesarios. Amazon Inspector produce una puntuación numérica del 1 al 10 que refleja la gravedad de la vulnerabilidad. Amazon Inspector la categoriza como una puntuación base porque refleja la gravedad de una vulnerabilidad según sus características intrínsecas, que son constantes a lo largo del tiempo. Esta puntuación también asume el peor impacto posible que puede esperarse en distintos entornos implementados. El estándar CVSS v3 asigna puntuaciones CVSS a las siguientes clasificaciones de gravedad.

Puntuación	Clasificación
0	Informational
0.1–3.9	Low
4.0–6.9	Medium
7.0–8.9	High
9.0–10.0	Critical

Los hallazgos de vulnerabilidad de paquetes también pueden tener asignado el valor de gravedad No evaluada. Esto significa que el proveedor aún no ha establecido una puntuación para la vulnerabilidad detectada. En este caso, recomendamos utilizar las direcciones URL de referencia del hallazgo para investigar la vulnerabilidad y actuar en consecuencia.

Los hallazgos de vulnerabilidad de paquetes incluyen las siguientes puntuaciones y los vectores de puntuación asociados en los detalles del hallazgo:

- Puntuación de EPSS
- Puntuación de Inspector
- CVSS 3.1 de CVE de Amazon
- CVSS 3.1 de NVD

- CVSS 2.0 de NVD (si procede)

Gravedad de una vulnerabilidad de código

Para detectar vulnerabilidades en el código, Amazon Inspector utiliza los niveles de gravedad definidos por los CodeGuru detectores de Amazon que generaron el hallazgo. A cada detector se le asigna una gravedad mediante el sistema de puntuación CVSS v3. Para obtener una explicación de los tipos de gravedad utilizados CodeGuru , consulte las definiciones de gravedad en la CodeGuru guía. Para ver una lista de detectores por nivel de gravedad, seleccione uno de los siguientes lenguajes de programación compatibles:

- Detectores de Python por nivel de gravedad
- Detectores de Java por nivel de gravedad

Gravedad de una vulnerabilidad de accesibilidad de red

Amazon Inspector determina la gravedad de una vulnerabilidad de accesibilidad de red en función del servicio, los puertos y los protocolos expuestos y del tipo de ruta abierta. Las clasificaciones de gravedad se definen en la tabla que verá a continuación. El valor de la columna de clasificación de rutas abiertas representa las rutas abiertas desde puertas de enlace virtuales, VPC interconectadas y redes. AWS Direct Connect El resto de servicios, puertos y protocolos expuestos tienen una clasificación de gravedad informativa.

Servicio	Puertos TCP	Puertos UDP	Clasificación de la ruta a Internet	Clasificación de la ruta abierta
DHCP	67, 68, 546, 547	67, 68, 546, 547	Medium	Informational
Elasticsearch	9300, 9200	NA	Medium	Informational
FTP	21	21	High	Medium
Global catalog LDAP	3268	NA	Medium	Informational
Global catalog LDAP over TLS	3269	NA	Medium	Informational

HTTP	80	80	Low	Informational
HTTPS	443	443	Low	Informational
Kerberos	88, 464, 543, 544, 749, 751	88, 464, 749, 750, 751, 752	Medium	Informational
LDAP	389	389	Medium	Informational
LDAP over TLS	636	NA	Medium	Informational
MongoDB	27017, 27018, 27019, 28017	NA	Medium	Informational
MySQL	3306	NA	Medium	Informational
NetBIOS	137, 139	137, 138	Medium	Informational
NFS	111, 2049, 4045, 1110	111, 2049, 4045, 1110	Medium	Informational
Oracle	1521, 1630	NA	Medium	Informational
PostgreSQL	5432	NA	Medium	Informational
Print services	515	NA	High	Medium
RDP	3389	3389	Medium	Low
RPC	111, 135, 530	111, 135, 530	Medium	Informational
SMB	445	445	Medium	Informational
SSH	22	22	Medium	Low
SQL Server	1433	1434	Medium	Informational
Syslog	601	514	Medium	Informational
Telnet	23	23	High	Medium
WINS	1512, 42	1512, 42	Medium	Informational

Administración de los hallazgos en Amazon Inspector

Amazon Inspector ofrece varias formas de ordenar, agrupar y administrar los hallazgos. Estas funciones le ayudan a adaptar los hallazgos a su entorno, agrupar los hallazgos según diferentes puntos de vista y centrarse en las vulnerabilidades de su AWS entorno específico.

Los hallazgos aparecen en distintas vistas en función de su estado, que puede ser Activo, Suprimido o Cerrado. De forma predeterminada, cada visa muestra únicamente los hallazgos activos. Un hallazgo activo representa un posible problema de seguridad detectado por Amazon Inspector para informar de una vulnerabilidad o una amenaza potencial. Los hallazgos suprimidos son hallazgos activos que se han excluido mediante reglas de supresión. Amazon Inspector establece automáticamente el estado de un hallazgo como cerrado cuando detecta que el hallazgo se ha corregido. Los hallazgos no se pueden cerrar manualmente.

También puede ver los resultados en AWS Security Hub un servicio que proporciona una visión integral del estado de la seguridad en todo el AWS entorno. Para obtener más información, consulte Integración de Amazon Inspector con AWS Security Hub. Los hallazgos de imágenes de contenedores también están disponibles en la consola de Amazon ECR, y puede ver los hallazgos de todos los recursos mediante AWS Command Line Interface (AWS CLI) o la API.

Temas

Visualización de los hallazgos de Amazon Inspector

La consola de Amazon Inspector muestra los hallazgos en vistas de pestañas según agrupaciones relacionadas. Cada vista incluye información que puede ayudarle a analizar vulnerabilidades específicas, a identificar los recursos más vulnerables y a medir el impacto general de las vulnerabilidades en el entorno. Para acceder a una vista de hallazgos distinta, elija la opción que se encuentra debajo del panel lateral de navegación Hallazgos. También puede crear un filtro en cada

vista para centrarse en tipos de hallazgos específicos. Para obtener más información acerca de los filtros, consulte Filtrado de hallazgos de Amazon Inspector.

Los hallazgos se pueden agrupar en función de los siguientes parámetros:

- Por vulnerabilidad: enumera las vulnerabilidades más críticas que se han detectado en el entorno. Elija un título de vulnerabilidad de esta vista para abrir un panel de detalles con información adicional.
- Por cuenta: enumera las cuentas, el porcentaje de cobertura de análisis de Amazon Inspector para cada cuenta y el número total de hallazgos de gravedad crítica y alta en cada cuenta. Esta agrupación solo está disponible para los administradores delegados.
- Por instancia: enumera las instancias de Amazon EC2 más vulnerables del entorno.
- Por imagen de contenedor: enumera las imágenes de contenedores de Amazon ECR más vulnerables del entorno.
- Por repositorio de contenedor: muestra los repositorios con más vulnerabilidades.
- Por función de Lambda: muestra las funciones de Lambda con más vulnerabilidades.
- Todos los hallazgos: muestra una lista completa con todos los hallazgos del entorno. Esta es la vista que se muestra de forma predeterminada cuando accede a la página Hallazgos. En esta vista, puede filtrar por hallazgos activos, suprimidos y cerrados.

Puede crear reglas de supresión basadas en filtros para excluir hallazgos de las vistas de hallazgos. Para obtener más información, consulte Supresión de hallazgos de Amazon Inspector mediante reglas de supresión.

Filtrado de hallazgos de Amazon Inspector

Un filtro de hallazgos le permite ver únicamente los hallazgos que coinciden con los criterios que especifique. Los hallazgos que no coinciden con los criterios de filtro se excluyen de la vista. Puede crear filtros de hallazgos con la consola de Amazon Inspector. Para obtener información sobre cómo utilizar los filtros con el fin de suprimir automáticamente los hallazgos existentes y futuros, consulte Supresión de hallazgos de Amazon Inspector mediante reglas de supresión.

Creación de filtros en la consola de Amazon Inspector

En cada vista de hallazgos, puede utilizar la funcionalidad de filtrado para encontrar hallazgos con características concretas. Los filtros se eliminan al desplazarse a una vista de pestaña diferente.

Un filtro se compone de un criterio de filtro, que consiste en un atributo de filtro emparejado con un valor de filtro. Los hallazgos que no coinciden con los criterios de filtro se excluyen de la vista. Por ejemplo, para ver todos los resultados asociados a su cuenta de administrador, puede elegir el atributo de ID de AWS cuenta y asociarlo con el valor de su ID de AWS cuenta de doce dígitos.

Algunos criterios de filtro se aplican a todos los hallazgos, mientras que otros solo están disponibles para determinados tipos de recurso o de hallazgo.

Aplicación de un filtro a la vista de hallazgos

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. En el panel de navegación, seleccione Findings (resultados). En la vista predeterminada se muestran todos los hallazgos con el estado Activo.
3. Para filtrar los hallazgos por criterio, seleccione la barra Agregar filtro. Se mostrará una lista de todos los criterios de filtro aplicables a esa vista. Los criterios de filtro pueden variar en función de la vista.
4. Elija un criterio que desee aplicar como filtro de la lista.
5. En el panel de entrada de criterios, introduzca los valores de filtro para definir ese criterio.
6. Elija Aplicar para aplicar el criterio de filtro a los resultados actuales. Para seguir agregando criterios de filtro, seleccione la barra de entrada de filtros de nuevo.
7. (Opcional) Para ver los filtros suprimidos o cerrados, elija Activo en la barra de filtros y, a continuación, elija Suprimido o Cerrado. Elija Mostrar todo para ver los hallazgos activos, suprimidos y cerrados en la misma vista.

Supresión de hallazgos de Amazon Inspector mediante reglas de supresión

Utilice las reglas de supresión para excluir los hallazgos que coincidan con los criterios. Por ejemplo, puede crear una regla que suprima todos los hallazgos con puntuaciones de vulnerabilidad bajas, de modo que pueda centrarse únicamente en los hallazgos más críticos.

> **Note**
>
> Las reglas de supresión solo se utilizan para filtrar la lista de hallazgos y no tienen ningún impacto en los hallazgos ni impiden que Amazon Inspector genere hallazgos.

Si Amazon Inspector genera hallazgos que coinciden con una regla de supresión, los hallazgos se configuran como Eliminados. Los hallazgos que coinciden con una regla de supresión no aparecen en la lista de forma predeterminada.

Amazon Inspector almacena los hallazgos suprimidos hasta que se corrijan. Amazon Inspector detecta los hallazgos corregidos. Cuando Amazon Inspector detecta un hallazgo subsanado, lo pone en Cerrado y lo guarda durante 7 días.

Los hallazgos suprimidos se AWS Security Hub publican en Amazon EventBridge como eventos. Puede suprimir automáticamente los hallazgos no deseados en Security Hub cambiando el estado de los hallazgos mediante una EventBridge regla. Para obtener más información, consulte Cómo crear reglas de supresión automática en AWS Security Hub.

No puede crear una regla de supresión que cierre o corrija los hallazgos. Solo puede crear una regla de supresión para filtrar los hallazgos que aparecen en su lista. Puede consultar los hallazgos suprimidos en cualquier momento desde la consola de Amazon Inspector.

> **Note**
>
> Las cuentas de los miembros de una organización no pueden crear ni administrar reglas de supresión.

Creación de una regla de supresión

Puede crear reglas de supresión para filtrar los hallazgos que se muestran de forma predeterminada en la lista. Puedes crear una regla de supresión mediante programación mediante la CreateFilterAPI y especificándola `SUPRESS` como valor para. `action`

> **Note**
>
> Solo las cuentas independientes y los administradores delegados de Amazon Inspector pueden crear y administrar reglas de supresión. Los miembros de una organización no verán la opción de reglas de supresión en el panel de navegación.

Creación de una regla de supresión (consola)

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.

2. En el panel de navegación, elija Reglas de supresión. A continuación, elija Crear regla.
3. Para cada criterio, haga lo siguiente:
   - Seleccione la barra de filtro para ver una lista de los criterios de filtro que puede agregar a la regla de supresión.
   - Seleccione los criterios de filtro que quiera agregar a la regla de supresión.
4. Una vez que haya acabado de agregar criterios, escriba el nombre de la regla y una descripción opcional.
5. Seleccione Guardar regla. Amazon Inspector aplica inmediatamente la nueva regla de supresión y oculta todos los hallazgos que coinciden con los criterios.

Visualización de hallazgos suprimidos

De forma predeterminada, Amazon Inspector no muestra los hallazgos suprimidos en la consola de Amazon Inspector. No obstante, puede verlos si utiliza una regla particular.

Visualización de hallazgos suprimidos

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. En el panel de navegación, seleccione Reglas de supresión.
3. En la lista de reglas de supresión, seleccione el título de la regla.

Modificación de reglas de supresión

Puede realizar cambios en las reglas de supresión en cualquier momento.

Modificación de reglas de supresión

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. En el panel de navegación, seleccione Reglas de supresión.
3. Seleccione el título de la regla de supresión que quiera modificar.
4. Realice los cambios correspondientes y elija Guardar para actualizar la regla.

Eliminación de reglas de supresión

Las reglas de supresión se pueden eliminar. Al eliminar una regla de supresión, Amazon Inspector deja de suprimir los hallazgos nuevos y existentes que cumplen con los criterios de la regla y que no están suprimidos por otras reglas.

Después de eliminar una regla de supresión, los hallazgos nuevos y existentes que cumplían con los criterios de la regla pasan al estado Activo. Esto significa que vuelven a aparecer de forma predeterminada en la consola de Amazon Inspector. Además, Amazon Inspector publica estas conclusiones en AWS Security Hub y Amazon EventBridge como eventos.

Eliminación de una regla de supresión

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. En el panel de navegación, seleccione Reglas de supresión.
3. Marque la casilla que se encuentra al lado del título de la regla de supresión que quiere eliminar.
4. Elija Eliminar y, a continuación, confirme la elección para eliminar la regla permanentemente.

Exportación de informes de hallazgos de Amazon Inspector

Además de enviar hallazgos a Amazon EventBridge y a AWS Security Hub, también puede exportar los hallazgos a un bucket de Amazon Simple Storage Service (Amazon S3) en forma de informe de hallazgos. Un informe de hallazgos es un archivo CSV o JSON que contiene los detalles de los hallazgos que ha elegido incluir en el informe. Proporciona una instantánea detallada de los hallazgos en un momento específico. Para cada hallazgo, en el archivo se incluyen detalles como el nombre de recurso de Amazon (ARN) del recurso afectado, la fecha y hora en la que se creó el hallazgo, el ID de Vulnerabilidades y riesgos comunes (CVE) asociado, la gravedad del hallazgo, su estado y las puntuaciones de Amazon Inspector y CVSS.

Para comenzar a configurar un informe de hallazgos, debe especificar los hallazgos que desea incluir en el informe. De forma predeterminada, Amazon Inspector incluye los datos de todos los hallazgos en la Región de AWS actual que tienen el estado Activo. Si es administrador delegado de Amazon Inspector de una organización, se incluyen, además, datos de los hallazgos de todas las cuentas de miembros de la organización.

Si lo desea, puede filtrar los datos de un informe para personalizarlo. Los filtros le permiten incluir o excluir datos de hallazgos con características concretas como, por ejemplo, todos los hallazgos críticos que se crearon durante un intervalo de tiempo específico, todos los hallazgos activos de un

recurso o todos los hallazgos críticos de un tipo específico. Si es administrador delegado de Amazon Inspector de una organización, puede utilizar los filtros para crear un informe que incluya hallazgos de una Cuenta de AWS específica de la organización. Por ejemplo, puede crear un informe con todos los hallazgos críticos de una cuenta con el estado activo para los que haya una corrección disponible. A continuación, puede compartir el informe con el propietario de la cuenta para que solucione el problema.

> **Note**
>
> Al exportar un informe de hallazgos con la API CreateFindingsReport, solo se muestran los hallazgos activos de forma predeterminada. Para ver los hallazgos suprimidos o cerrados, debe especificar `SUPPRESSED` o `CLOSED` valores en el criterio de filtro findingStatus.

Al exportar un informe de hallazgos, Amazon Inspector cifra los datos con una clave de AWS Key Management Service (AWS KMS) de su elección y agrega el informe al bucket de S3 que haya especificado. La clave de cifrado debe ser una clave de cifrado simétrico de AWS Key Management Service (AWS KMS) administrada por el cliente que se encuentre en la Región de AWS actual. Asimismo, la política de claves debe permitir que Amazon Inspector utilice la clave. El bucket S3 también debe estar en la región actual y la política del bucket debe permitir que Amazon Inspector agregue objetos al bucket.

Cuando Amazon Inspector ha acabado de cifrar y almacenar el informe, este se puede descargar desde el bucket de S3 que ha especificado o moverse a otra ubicación. También puede mantener el informe en el bucket de S3 y utilizar el bucket como repositorio para todos los informes de hallazgos que exporte más adelante.

En esta sección se explica cómo utilizar la AWS Management Console para exportar un informe de hallazgos. El proceso consiste en verificar que cuenta con los permisos necesarios, configurar los recursos necesarios y, por último, configurar y exportar el informe.

> **Note**
>
> Solo puede exportar un informe de hallazgos a la vez. Si ya se está exportando un informe, espere a que se acabe de exportar antes de exportar otro informe.

Tareas

Tras exportar un informe de hallazgos por primera vez, los pasos del 1 al 3 son opcionales. Esto depende de si quiere utilizar el mismo bucket de S3 y AWS KMS key para próximos informes.

Si prefiere exportar un informe programáticamente tras seguir los pasos del 1 al 3, utilice la operación CreateFindingsReport de la API de Amazon Inspector.

Paso 1: verificación de permisos

Antes de exportar un informe de hallazgos de Amazon Inspector, debe verificar que cuenta con todos los permisos necesarios para exportar informes de hallazgos y configurar recursos de cifrado y almacenamiento de informes. Para verificar sus permisos, utilice AWS Identity and Access Management (IAM) para revisar las políticas de IAM asociadas a su identidad de IAM. A continuación, debe comparar la información de estas políticas con la siguiente lista de acciones que debe poder realizar para exportar un informe de hallazgos.

Amazon Inspector

Para Amazon Inspector, verifique que tiene permiso para realizar las siguientes acciones:

- `inspector2:ListFindings`
- `inspector2:CreateFindingsReport`

Estas acciones le permiten obtener datos de hallazgos de su cuenta y exportarlos en forma de informes de hallazgos.

Si tiene pensado exportar grandes informes programáticamente, se recomienda verificar los permisos para realizar las siguientes acciones: `inspector2:GetFindingsReportStatus`, que comprueba el estado de los informes; y `inspector2:CancelFindingsReport`, que cancela las exportaciones en curso.

AWS KMS

Para AWS KMS, verifique que tiene permiso para realizar las siguientes acciones:

- `kms:GetKeyPolicy`
- `kms:PutKeyPolicy`

Estas acciones le permiten obtener y actualizar la política de claves de la clave de AWS KMS key que quiere utilizar con Amazon Inspector para cifrar el informe.

Antes de utilizar la consola de Amazon Inspector para exportar un informe, tiene que verificar que puede realizar las siguientes acciones de AWS KMS:

- `kms:DescribeKey`
- `kms:ListAliases`

Estas acciones le permiten obtener y mostrar información sobre las AWS KMS keys de la cuenta. A continuación, puede elegir una de esas claves para cifrar el informe.

Si tiene pensado crear una nueva clave de KMS para cifrar informes, debe tener permisos para realizar la acción `kms:CreateKey`.

Amazon S3

Para Amazon S3, verifique que tiene permiso para realizar las siguientes acciones:

- `s3:CreateBucket`
- `s3:DeleteObject`
- `s3:PutBucketAcl`
- `s3:PutBucketPolicy`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutObject`
- `s3:PutObjectAcl`

Estas acciones le permiten crear y configurar el bucket de S3 donde desea que Amazon Inspector almacene el informe. También le permiten agregar objetos al bucket y eliminarlos.

Si tiene pensado utilizar la consola de Amazon Inspector para exportar un informe, tiene que verificar que puede realizar las acciones de `s3:ListAllMyBuckets` y `s3:GetBucketLocation`: Estas acciones le permiten obtener y mostrar información sobre los buckets de S3 de la cuenta. A continuación, puede elegir uno de esos buckets para almacenar el informe.

Si no puede realizar una o más de las acciones necesarias, pida ayuda al administrador de AWS antes de avanzar al siguiente paso.

Paso 2: configuración de un bucket de S3

Una vez que haya verificado sus permisos, podrá configurar el bucket de S3 donde desea almacenar el informe de hallazgos. Puede ser un bucket de su propia cuenta o un bucket propiedad de otra Cuenta de AWS al que pueda acceder. Si desea almacenar un informe en un nuevo bucket, créelo antes de continuar.

El bucket de S3 debe encontrarse en la misma Región de AWS que los datos de hallazgos que desea exportar. Por ejemplo, si utiliza Amazon Inspector en la región Este de EE. UU. (Norte de Virginia) y desea exportar los datos de hallazgos para esa región, el bucket también debe estar en la región Este de EE. UU. (Norte de Virginia).

Además, la política del bucket debe permitir a Amazon Inspector agregar objetos al bucket. En esta sección se explica cómo actualizar la política del bucket y se incluye un ejemplo de la instrucción que tiene que agregar a la política. Para obtener información detallada sobre cómo agregar y actualizar políticas de buckets, consulte Uso de políticas de bucket en la Guía del usuario de Amazon Simple Storage Service.

Si quiere almacenar el informe en un bucket de S3 propiedad de otra cuenta, colabore con el propietario del bucket para actualizar la política del bucket. También debe obtener el URI del bucket para introducirlo cuando exporte el informe.

Actualización de la política del bucket

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación, elija Buckets.
3. Elija el bucket de S3 donde desea almacenar el informe de hallazgos.
4. Elija la pestaña Permissions (Permisos).
5. Elija Editar en la sección Política de bucket.
6. Copie la siguiente instrucción de muestra en el portapapeles:

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

```
    "Sid": "allow-inspector",
    "Effect": "Allow",
    "Principal": {
     "Service": "inspector2.amazonaws.com"
    },
    "Action": [
     "s3:PutObject",
     "s3:PutObjectAcl",
     "s3:AbortMultipartUpload"
    ],
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
    "Condition": {
     "StringEquals": {
      "aws:SourceAccount": "111122223333"
     },
     "ArnLike": {
      "aws:SourceArn": "arn:aws:inspector2:Region:111122223333:report/*"
     }
    }
   }
  ]
}
```

7. En el editor de políticas de buckets de la consola de Amazon S3, pegue la instrucción anterior en la política para agregarla a la política.

   Cuando agregue la instrucción, asegúrese de que la sintaxis sea válida. Las políticas de buckets utilizan el formato JSON. Esto significa que tiene que insertar una coma al principio o al final de la instrucción, dependiendo del lugar de la política al que agregue la instrucción. Si agrega la instrucción como la última instrucción, inserte la coma después del corchete de cierre de la instrucción anterior. Si la agrega como primera instrucción o entre dos instrucciones existentes, inserte la coma después del corchete de cierre de la instrucción que acaba de agregar.

8. Actualice la instrucción con los valores correctos para su entorno:

   - *DOC-EXAMPLE-BUCKET* es el nombre del bucket.
   - *111122223333* es el ID de la Cuenta de AWS.
   - *Region* es la Región de AWS en la que utiliza Amazon Inspector y en la que quiere permitir que Amazon Inspector agregue informes al bucket. Por ejemplo, `us-east-1` es la región Este de EE. UU. (Norte de Virginia).

> **Note**
>
> Si utiliza Amazon Inspector en una Región de AWS habilitada manualmente, agregue el código de región correspondiente al valor del campo `Service`. En este campo se especifica la entidad principal del servicio Amazon Inspector.
> Por ejemplo, si utiliza Amazon Inspector en la región Medio Oriente (Baréin), cuyo código de región es `me-south-1`, cambie `inspector2.amazonaws.com` por `inspector2.me-south-1.amazonaws.com` en la instrucción.

Tenga en cuenta que la instrucción de muestra define las condiciones que utilizan dos claves de condición globales de IAM:

- aws:SourceAccount: esta condición permite a Amazon Inspector agregar informes únicamente de su cuenta al bucket. Impide que Amazon Inspector agregue informes de otras cuentas al bucket. Más concretamente, la condición especifica la cuenta que puede utilizar el bucket para los recursos y acciones que se definen en la condición `aws:SourceArn`.

  Para almacenar informes de otras cuentas en el bucket, agregue el ID de cuenta de todas las cuentas adicionales a esta condición. Por ejemplo:

  ```
  "aws:SourceAccount": [111122223333,444455556666,123456789012]
  ```

- aws:SourceArn: esta condición restringe el acceso al bucket en función del origen de los objetos que se han agregado al bucket. Impide que otros Servicios de AWS agreguen objetos al bucket. También impide que Amazon Inspector agregue objetos al bucket mientras se llevan a cabo otras acciones en su cuenta. Más concretamente, la condición permite a Amazon Inspector agregar objetos al bucket únicamente si los objetos son informes de hallazgos y si estos informes se han creado en la cuenta y en la región que se indican en la condición.

  Para permitir que Amazon Inspector realice las acciones especificadas en cuentas distintas, agregue los nombres de recursos de Amazon (ARN) de cada cuenta adicional a esta condición. Por ejemplo:

  ```
  "aws:SourceArn": [
      "arn:aws:inspector2:Region:111122223333:report/*",
      "arn:aws:inspector2:Region:444455556666:report/*",
  ```

```
    "arn:aws:inspector2:Region:123456789012:report/*"
]
```

Las cuentas que se especifican en las condiciones `aws:SourceAccount` y `aws:SourceArn` deberían coincidir.

Ambas condiciones ayudan a evitar que Amazon Inspector se utilice como suplente confuso durante las transacciones con Amazon S3. Aunque no se recomienda, puede eliminar estas condiciones de la política del bucket.

9. Cuando haya terminado de actualizar la política del bucket, elija Guardar cambios.

Paso 3: configuración de una AWS KMS key

Una vez que hayan verificado los permisos y haya configurado el bucket de S3, elija la AWS KMS key que quiera utilizar en Amazon Inspector para cifrar el informe de hallazgos. La clave debe ser una clave de KMS de cifrado simétrico administrada por el cliente. Además, la clave debe estar en la misma Región de AWS que el bucket de S3 que ha configurado para almacenar el informe.

La clave puede ser una clave de KMS de su propia cuenta o una clave de KMS propiedad de otra cuenta. Si quiere utilizar una clave de KMS nueva, cree la clave antes de continuar. Si desea utilizar una clave existente propiedad de otra cuenta, debe obtener el nombre de recurso de Amazon (ARN) de la clave. Tendrá que ingresar este ARN cuando exporte el informe de Amazon Inspector. Para obtener información sobre cómo crear y revisar la configuración de las claves de KMS, consulte Administración de claves en la Guía del desarrollador de AWS Key Management Service.

Una vez que haya determinado la clave de KMS que quiere utilizar, conceda permiso a Amazon Inspector para que utilice la clave. De lo contrario, Amazon Inspector no podrá cifrar ni exportar el informe. Para conceder permiso a Amazon Inspector para que utilice la clave, actualice la política de claves de la clave. Para obtener información detallada acerca de las políticas de claves y la gestión del acceso a claves de KMS, consulte Políticas de claves en AWS KMS en la Guía del desarrollador de AWS Key Management Service.

Actualización de la política de claves

> **Note**
>
> El siguiente procedimiento sirve para actualizar una clave para que Amazon Inspector pueda utilizarla. Si no tiene una clave, consulte https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html para obtener información sobre cómo crear una clave.

1. Abra la consola de AWS KMS en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.
4. Elija la clave de KMS que quiera utilizar para cifrar el informe. La clave debe ser una clave de cifrado simétrico (SYMMETRIC_DEFAULT).
5. En la pestaña Política de claves, elija Editar. Si no ve una política de claves con el botón Editar, primero debe seleccionar Cambiar a vista de política.
6. Copie la siguiente instrucción de muestra en el portapapeles:

```
{
    "Sid": "Allow Amazon Inspector to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "inspector2.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:inspector2:Region:111122223333:report/*"
        }
    }
}
```

7. En el editor de políticas de claves de la consola de AWS KMS, pegue la instrucción anterior en la política de claves para agregarla a la política.

   Cuando agregue la instrucción, asegúrese de que la sintaxis sea válida. Las políticas de claves utilizan el formato JSON. Esto significa que tiene que insertar una coma al principio o al final de la instrucción, dependiendo del lugar de la política al que agregue la instrucción. Si agrega la instrucción como la última instrucción, inserte la coma después del corchete de cierre de la instrucción anterior. Si la agrega como primera instrucción o entre dos instrucciones existentes, inserte la coma después del corchete de cierre de la instrucción que acaba de agregar.

8. Actualice la instrucción con los valores correctos para su entorno:

   - *111122223333* es el ID de la Cuenta de AWS.
   - *Region* es la Región de AWS en la que desea permitir que Amazon Inspector cifre informes con la clave. Por ejemplo, `us-east-1` es la región Este de EE. UU. (Norte de Virginia).

   > **Note**
   >
   > Si utiliza Amazon Inspector en una Región de AWS habilitada manualmente, agregue el código de región correspondiente al valor del campo `Service`. Por ejemplo, si utiliza Amazon Inspector en la región Medio Oriente (Baréin), sustituya `inspector2.amazonaws.com` por `inspector2.me-south-1.amazonaws.com`.

   Igual que en la instrucción de muestra para la política del bucket del paso anterior, los campos `Condition` de este ejemplo utilizan dos claves de condición globales de IAM:

   - aws:SourceAccount: esta condición permite a Amazon Inspector realizar las acciones especificadas únicamente en su cuenta. Más concretamente, determina la cuenta que puede realizar las acciones especificadas para los recursos y acciones que se definen en la condición `aws:SourceArn`.

     Para permitir que Amazon Inspector realice las acciones especificadas en cuentas distintas, agregue los ID de cuenta de cada cuenta adicional a esta condición. Por ejemplo:

     ```
     "aws:SourceAccount": [111122223333,444455556666,123456789012]
     ```

   - aws:SourceArn: esta condición evita que otros Servicios de AWS realicen las acciones especificadas. También impide que Amazon Inspector utilice la clave mientras se llevan a

cabo otras acciones en su cuenta. Más concretamente, permite a Amazon Inspector cifrar objetos de S3 con la clave únicamente si los objetos son informes de hallazgos y si estos informes se han creado en la cuenta y en la región que se indican en la condición.

Para permitir que Amazon Inspector realice las acciones especificadas en cuentas distintas, agregue los ARN de cada cuenta adicional a esta condición. Por ejemplo:

```
"aws:SourceArn": [
    "arn:aws:inspector2:us-east-1:111122223333:report/*",
    "arn:aws:inspector2:us-east-1:444455556666:report/*",
    "arn:aws:inspector2:us-east-1:123456789012:report/*"
]
```

Las cuentas que se especifican en las condiciones `aws:SourceAccount` y `aws:SourceArn` deberían coincidir.

Estas condiciones ayudan a evitar que Amazon Inspector se utilice como suplente confuso durante las transacciones con AWS KMS. Aunque no se recomienda, puede eliminar estas condiciones de la instrucción.

9. Cuando haya terminado de actualizar la política de claves, elija Guardar cambios.

Paso 4: configuración y exportación de un informe de hallazgos

Una vez que haya verificado los permisos y configurado los recursos que quiere cifrar y almacenar en el informe de hallazgos, podrá configurar y exportar el informe.

Configuración y exportación de un informe de hallazgos

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. En el panel de navegación, en Hallazgos, elija Todos los hallazgos.
3. (Opcional) Con la barra de filtros ubicada sobre la tabla Hallazgos, agregue los criterios de filtro necesarios para definir los hallazgos que se incluirán en el informe. A medida que agrega criterios, Amazon Inspector actualiza la tabla para incluir únicamente los hallazgos que coinciden con los criterios. La tabla proporciona una vista previa de los datos que contendrá el informe.

> **Note**
>
> Le recomendamos que agregue criterios de filtro. De lo contrario, el informe incluirá datos de todos los hallazgos de la Región de AWS actual que tengan el estado Activo. Si es administrador de Amazon Inspector de una organización, se incluyen, además, datos de los hallazgos de todas las cuentas de miembros de la organización.
> Si un informe incluye datos de demasiados hallazgos o de todos, tardará más tiempo en generarse y exportarse. Tenga en cuenta que solo puede exportar un informe a la vez.

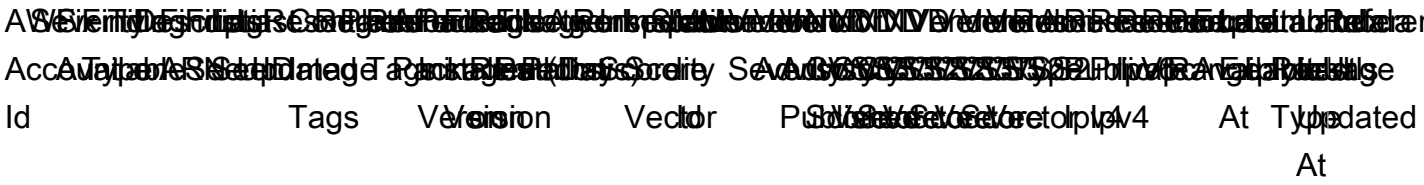
4. Elija Exportación de hallazgos.
5. En la sección Configuración de exportación, para Tipo de archivo de exportación, especifique el formato de archivo del informe:

   - Para crear un archivo JavaScript Object Notation (.json) que contenga los datos, elija JSON.

     Si elige la opción JSON, el informe incluirá todos los campos de cada hallazgo. Para ver una lista de los posibles campos de un archivo JSON, consulte el tipo de datos Hallazgo en la referencia de la API de Amazon Inspector.

   - Para crear un archivo de valores separados por comas (.csv) que contenga los datos, elija CSV.

     Si elige la opción CSV, el informe incluirá únicamente un subconjunto de los campos de cada hallazgo; es decir, aproximadamente 45 campos que informan de los atributos clave de un hallazgo. Algunos de los campos incluidos son Tipo de hallazgo, Título, Gravedad, Estado, Descripción, Visto por primera vez, Visto por última vez, Corrección disponible, ID de cuenta de AWS, ID de recurso, Etiquetas de recursos y Corrección. Estos campos se suman a los campos que recopilan detalles de puntuaciones y URL de referencia de cada hallazgo. La siguiente tabla muestra los encabezados CSV de un informe de resultados:



6. En Ubicación de la exportación, para URI de S3, especifique el bucket de S3 donde desea almacenar el informe:

- Para almacenar el informe en un bucket de su cuenta, elija Explorar S3. Amazon Inspector muestra una tabla con los buckets de S3 de la cuenta. Seleccione la fila del bucket que quiera utilizar y, a continuación, elija Elegir.

  > **Tip**
  >
  > Para especificar un prefijo de ruta de Amazon S3 en el informe, agregue una barra inclinada (/) y el prefijo al principio del valor en el cuadro URI de S3. A continuación, Amazon Inspector incluye el prefijo cuando agrega el informe al bucket y Amazon S3 genera la ruta que especifica el prefijo.
  > Por ejemplo, si quiere utilizar el ID de Cuenta de AWS ID como prefijo y el ID de la cuenta es 111122223333, agregue **`/111122223333`** al principio del valor en el cuadro URI de S3.
  > Un prefijo se parece a una ruta de directorio en un bucket de S3. Le permite agrupar objetos similares en un bucket, de la misma forma que clasificaría archivos en una carpeta de un sistema de archivos. Para obtener más información, consulte Organización de objetos en la consola de Amazon S3 con carpetas en la Guía del usuario de Amazon Simple Storage Service.

- Para almacenar el informe en un bucket propiedad de otra cuenta, introduzca el URI del bucket. Un ejemplo de URI es **`s3://DOC-EXAMPLE_BUCKET`**, donde DOC-EXAMPLE_BUCKET es el nombre del bucket. El propietario del bucket puede buscar esta información en las propiedades del bucket.

7. En Clave de KMS, especifique la AWS KMS key que quiera utilizar para cifrar el informe:

   - Para utilizar una clave de su cuenta, elija una clave de la lista. En la lista se muestran las claves de KMS de cifrado simétrico administradas por el cliente de la cuenta.
   - Para utilizar una clave propiedad de otra cuenta, introduzca el nombre de recurso de Amazon (ARN) de la clave. El propietario de la clave puede buscar esta información en las propiedades de la clave. Para obtener más información, consulte Búsqueda del ID y el ARN de la clave en la Guía del desarrollador de AWS Key Management Service.

8. Elija Export (Exportar).

Amazon Inspector genera el informe de hallazgos, lo cifra con la clave de KMS que ha especificado y lo agrega al bucket de S3 que ha especificado. Este proceso puede tardar varios minutos e incluso horas, dependiendo del número de hallazgos que haya elegido incluir en el informe. Cuando finaliza

la exportación, Amazon Inspector muestra un mensaje para informar de que el informe de hallazgos se ha exportado correctamente. También puede elegir Ver informe en el mensaje para acceder al informe en Amazon S3.

Tenga en cuenta que solo puede exportar un informe a la vez. Si ya se está exportando un informe, espere a que se acabe de exportar antes de exportar otro informe.

Solución de errores de exportación

Si se produce un error al intentar exportar un informe de hallazgos, Amazon Inspector muestra un mensaje para describir el error. Puede utilizar la información de esta sección como guía para identificar posibles causas y soluciones del error.

Por ejemplo, una posible solución es verificar que el bucket de S3 se encuentre en la Región de AWS actual y que la política del bucket permita a Amazon Inspector agregar objetos al bucket. También puede comprobar si la AWS KMS key está habilitada en la región actual y que la política de claves permite a Amazon Inspector utilizar la clave.

Una vez que haya corregido el error, vuelva a intentar exportar el informe.

Mensaje de error sobre crear varios informes a la vez

Si ha intentado crear un informe mientras Amazon Inspector generaba un informe, recibirá el mensaje de error Motivo: no puede haber varios informes en curso. Este error se produce porque Amazon Inspector solo puede generar un informe a la vez para una cuenta.

Para solucionar el problema, espere a que finalice la exportación del otro informe o cancele la exportación antes de solicitar un nuevo informe.

Puede comprobar el estado de un informe con la operación GetFindingsReportStatus, que devuelve el ID de cualquier informe que se esté generando.

Si lo necesita, puede utilizar el ID de informe que proporciona la operación `GetFindingsReportStatus` para cancelar una exportación en curso con la operación CancelFindingsReport.

Creación de respuestas personalizadas para hallazgos de Amazon Inspector con Amazon EventBridge

Amazon Inspector crea un evento de Amazon EventBridge para los hallazgos recién generados, los hallazgos recién agregados y los cambios en el estado de los hallazgos. Para el resto de acciones que no sean cambios en los campos `updatedAt` y `lastObservedAt`, se publicará un nuevo evento. Esto significa que se generan nuevos eventos para un hallazgo cuando toma medidas como reiniciar un recurso o cambiar las etiquetas asociadas a un recurso. No obstante, el identificador del hallazgo en el campo `id` sigue siendo el mismo. Los eventos se emiten en la medida de lo posible.

> **Note**
>
> Si tiene una cuenta de administrador delegado de Amazon Inspector, EventBridge publica los eventos en su cuenta y en la cuenta de miembro de la que proceden.

Gracias a los eventos de EventBridge con Amazon Inspector, puede automatizar las tareas para responder a los problemas de seguridad que han detectado los hallazgos de Amazon Inspector.

Amazon Inspector emite los eventos al bus de eventos predeterminado de la misma región. Esto significa que debe configurar las reglas de eventos en cada región en la que utiliza Amazon Inspector para consultar eventos.

Para recibir notificaciones sobre los hallazgos de Amazon Inspector en función de eventos de EventBridge, debe crear una regla de EventBridge y un destino para Amazon Inspector. Esta regla permite a EventBridge enviar al destino especificado en la regla notificaciones de todos los hallazgos que genera Amazon Inspector. Para obtener más información, consulte las reglas de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

Esquema de evento

A continuación se muestra un ejemplo del formato de un evento de EventBridge para un evento de hallazgo de EC2. Para ver esquemas de muestra de otros tipos de hallazgo o de evento, consulte Esquema de EventBridge.

```
{
    "version": "0",
    "id": "66a7a279-5f92-971c-6d3e-c92da0950992",
```

```
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T22:46:15Z",
    "region": "us-east-1",
    "resources": ["i-0c2a343f1948d5205"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "\n It was discovered that the sound subsystem in the Linux
 kernel contained a\n race condition in some situations. A local attacker could use
 this to cause\n a denial of service (system crash).",
        "exploitAvailable": "YES",
        "exploitabilityDetails": {
            "lastKnownExploitAt": "Oct 24, 2022, 11:08:59 PM"
        },
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "fixAvailable": "YES",
        "lastObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "packageVulnerabilityDetails": {
            "cvss": [{
                "baseScore": 4.7,
                "scoringVector": "CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H",
                "source": "NVD",
                "version": "3.1"
            }],
            "referenceUrls": ["https://lore.kernel.org/all/
CAFcO6XN7JDM4xSXGhtusQfS2mSBcx50VJKwQpCq=WeLt57aaZA@mail.gmail.com/", "https://
ubuntu.com/security/notices/USN-5792-1", "https://ubuntu.com/security/notices/
USN-5791-2", "https://ubuntu.com/security/notices/USN-5791-1", "https://ubuntu.com/
security/notices/USN-5793-2", "https://git.kernel.org/pub/scm/linux/kernel/git/
torvalds/linux.git/commit/?id=8423f0b6d513b259fdab9c9bf4aaa6188d054c2d", "https://
ubuntu.com/security/notices/USN-5793-1", "https://ubuntu.com/security/notices/
USN-5792-2", "https://ubuntu.com/security/notices/USN-5791-3", "https://ubuntu.com/
security/notices/USN-5793-4", "https://ubuntu.com/security/notices/USN-5793-3",
 "https://git.kernel.org/linus/8423f0b6d513b259fdab9c9bf4aaa6188d054c2d(6.0-rc5)",
 "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3303"],
            "relatedVulnerabilities": [],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2022/
CVE-2022-3303.html",
            "vendorCreatedAt": "Sep 27, 2022, 11:15:00 PM",
            "vendorSeverity": "medium",
            "vulnerabilityId": "CVE-2022-3303",
```

```
            "vulnerablePackages": [{
                "arch": "X86_64",
                "epoch": 0,
                "fixedInVersion": "0:5.15.0.1027.31~20.04.16",
                "name": "linux-image-aws",
                "packageManager": "OS",
                "remediation": "apt update && apt install --only-upgrade linux-image-
aws",
                "version": "5.15.0.1026.30~20.04.16"
            }]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b7ff1a8d69f1bb35",
                    "ipV4Addresses": ["172.31.85.212", "44.203.45.27"],
                    "ipV6Addresses": [],
                    "launchedAt": "Jan 19, 2023, 7:53:14 PM",
                    "platform": "UBUNTU_20_04",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0c2a343f1948d5205",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "CVE-2022-3303 - linux-image-aws",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 10:46:15 PM"
    }
}
```

Creación de una regla de EventBridge para recibir notificaciones de los hallazgos de Amazon Inspector

EventBridge le permite configurar alertas automatizadas sobre hallazgos que se envían a un centro de mensajería para incrementar la visibilidad de los hallazgos de Amazon Inspector. En esta sección se muestra cómo enviar alertas de hallazgos de gravedad `CRITICAL` y `HIGH` por correo electrónico, Slack o Amazon Chime. Aprenderá a configurar un tema en Amazon Simple Notification Service y, a continuación, conectarlo a una regla de eventos de EventBridge.

Paso 1. Configuración de un tema y un punto de conexión de Amazon SNS

Para configurar las alertas automatizadas, antes debe configurar un tema en Amazon Simple Notification Service y agregar un punto de conexión. Para obtener más información, consulte la guía de SNS.

Este procedimiento establece la ubicación donde desea enviar los datos de los hallazgos de Amazon Inspector. El tema de SNS se puede agregar a una regla de eventos de EventBridge durante la creación de la regla de eventos o después de dicha creación.

Email setup

Creación de un tema de SNS

1. Inicie sesión en la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En el panel de navegación, seleccione Temas y, a continuación, Crear tema.
3. En la sección Crear tema, seleccione Estándar. A continuación, escriba un nombre de tema, como **`Inspector_to_Email`**. Lo demás datos son opcionales.
4. Elija Create Topic (Crear tema). Se abrirá un nuevo panel con detalles sobre el tema que acaba de crear.
5. En la sección Suscripciones, seleccione Crear suscripción.
6. a. En el menú Protocolo, seleccione Correo electrónico.
   b. En el campo Punto de conexión, introduzca la dirección de correo electrónico en la que desea recibir las notificaciones.

> **Note**
>
> Una vez creada la suscripción, tendrá que confirmarla a través del cliente de correo electrónico.

c. Elija Crear una suscripción.

7. Busque el mensaje de suscripción en la bandeja de entrada y elija Confirmar suscripción.

Slack setup

Creación de un tema de SNS

1. Inicie sesión en la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En el panel de navegación, seleccione Temas y, a continuación, Crear tema.
3. En la sección Crear tema, seleccione Estándar. A continuación, escriba un nombre de tema, como **`Inspector_to_Slack`**. Lo demás datos son opcionales. Elija Crear tema para acabar de crear el punto de conexión.

Configuración de un cliente de AWS Chatbot

1. Vaya a la consola AWS Chatbot en https://console.aws.amazon.com/chatbot/.
2. En el panel Clientes configurados, seleccione Configurar un nuevo cliente.
3. Elija Slack y, a continuación, Guardar.

> **Note**
>
> Al elegir Slack, debe confirmar los permisos de AWS Chatbot para acceder a su canal. Para ello, seleccione permitir.

4. Seleccione Configurar un nuevo canal para abrir el panel de detalles de configuración.

   a. Escriba un nombre para el canal.

   b. En Canal de Slack, elija el canal que quiera utilizar.

   c. En Slack, haga clic con el botón secundario en el nombre del canal y seleccione Copiar enlace para copiar el ID de canal del canal privado.

d. En la AWS Management Console, en la ventana AWS Chatbot, pegue el ID que ha copiado de Slack en el campo ID de canal privado.

e. En Permisos, elija crear un rol de IAM con una plantilla, en el caso de que no tenga un rol.

f. Para las plantillas de Política, elija Permisos de notificación. Esta es la plantilla de política de IAM para AWS Chatbot. Esta política proporciona los permisos de lectura y de lista necesarios para las alarmas, los eventos y los registros de CloudWatch, así como para los temas de Amazon SNS.

g. En Políticas de barrera de protección del canal, elija AmazonInspector2ReadOnlyAccess.

h. Elija la región en la que ha creado anteriormente el tema de SNS y, a continuación, seleccione el tema de Amazon SNS que ha creado para enviar notificaciones al canal de Slack.

5. Seleccione Configure (Configurar).

Amazon Chime setup

Creación de un tema de SNS

1. Inicie sesión en la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En el panel de navegación, seleccione Temas y, a continuación, Crear tema.
3. En la sección Crear tema, seleccione Estándar. A continuación, escriba un nombre de tema, como **`Inspector_to_Chime`**. Lo demás datos son opcionales. Elija Crear tema para finalizar este proceso.

Configuración de un cliente de AWS Chatbot

1. Vaya a la consola AWS Chatbot en https://console.aws.amazon.com/chatbot/.
2. En el panel Clientes configurados, seleccione Configurar un nuevo cliente.
3. Elija Chime y, a continuación, Configurar para confirmar.
4. En el panel Detalles de configuración, introduzca un nombre para el canal.
5. En Amazon Chime, abra la sala de chat que desea utilizar.

a. Elija el icono de engranaje en la esquina superior derecha y elija Manage webhooks and bots (Administrar webhooks y bots).

b. Seleccione Copiar URL para copiar la URL del webhook a su portapapeles.

6. En la AWS Management Console, en la ventana AWS Chatbot, pegue la URL que ha copiado en el campo URL de webhook.
7. En Permisos, elija crear un rol de IAM con una plantilla, en el caso de que no tenga un rol.
8. Para las plantillas de Política, elija Permisos de notificación. Esta es la plantilla de política de IAM para AWS Chatbot. Proporciona los permisos de lectura y de lista necesarios para las alarmas, los eventos y los registros de CloudWatch, así como para los temas de Amazon SNS.
9. Elija la región en la que ha creado anteriormente el tema de SNS y, a continuación, seleccione el tema de Amazon SNS que ha creado para enviar notificaciones a la sala de Amazon Chime.
10. Seleccione Configure (Configurar).

Paso 2. Creación de una regla de EventBridge para los hallazgos de Amazon Inspector

1. Abra la consola de Amazon EventBridge en https://console.aws.amazon.com/events/.
2. Seleccione Reglas en el panel de navegación y, después, Crear regla.
3. Escriba un nombre y una descripción opcional de la regla.
4. Elija Regla con un patrón de eventos y, a continuación, Siguiente.
5. En el panel Patrón de eventos, elija Patrones personalizados (editor JSON).
6. Pegue el siguiente objeto JSON en el editor.

```
{
  "source": ["aws.inspector2"],
  "detail-type": ["Inspector2 Finding"],
  "detail": {
    "severity": ["HIGH", "CRITICAL"],
    "status": ["ACTIVE"]
  }
}
```

> **Note**
>
> Este patrón envía notificaciones sobre cualquier hallazgo de gravedad `CRITICAL` o `HIGH` que detecte Amazon Inspector.

Seleccione Siguiente cuando haya acabado de introducir el patrón del evento.

7. En la página Seleccionar destinos, elija Servicio de AWS. A continuación, en Seleccionar tipo de destino, elija Tema de SNS.
8. En Tema, seleccione el nombre del tema de SNS que ha creado en el paso 1. A continuación, elija Next.
9. Agregue más etiquetas si las necesita y elija Siguiente.
10. Revise la regla y, a continuación, elija Crear regla.

EventBridge para entornos de varias cuentas de Amazon Inspector

Si es administrador delegado de Amazon Inspector, se muestran reglas de EventBridge en su cuenta en función de los hallazgos aplicables procedentes de las cuentas de miembros. Si configura las notificaciones sobre hallazgos a través de EventBridge en la cuenta de administrador, tal como se indica en la sección anterior, recibirá notificaciones acerca de varias cuentas. En otras palabras, recibirá información de los hallazgos y eventos generados en cuentas de miembros, así como de los hallazgos y eventos generados en su propia cuenta.

Puede utilizar el valor `accountId` de los detalles del archivo JSON del hallazgo para identificar la cuenta de miembro de la que procede el hallazgo de Amazon Inspector.

Exportación de SBOM con Amazon Inspector

Puede utilizar la consola de Amazon Inspector o la API para generar listados de componentes de software (SBOM) de sus recursos. Una SBOM es un inventario anidado de todos los componentes de software de código abierto y de terceros de la base de código. Amazon Inspector proporciona SBOM de recursos específicos del entorno. Las SBOM exportadas de Amazon Inspector pueden ayudarle a obtener visibilidad sobre la información relacionada con el suministro de software, como los paquetes que utiliza con más frecuencia y las vulnerabilidades asociadas en toda la organización.

Puede exportar SBOM de todos los recursos compatibles que se están supervisando con Amazon Inspector. Puede revisar el estado de los recursos mediante la Evaluación de la cobertura de Amazon Inspector para el entorno de AWS.

> **Note**
>
> Amazon Inspector no admite la exportación de SBOM para instancias de EC2 de Windows.

Formatos de Amazon Inspector

Amazon Inspector admite la exportación de SBOM en los formatos CycloneDX 1.4 y SPDX 2.3 compatibles. Amazon Inspector exporta las SBOM como archivos `JSON` a un bucket de Amazon S3 de su elección.

> **Note**
>
> Las exportaciones en formato SPDX de Amazon Inspector son compatibles con los sistemas con SPDX 2.3. No obstante, no contienen el campo Creative Commons Zero (CC0). El motivo es que, si se incluyera este campo, los usuarios podrían redistribuir o editar el material.

Ejemplo del formato para SBOM de CycloneDX 1.4 de Amazon Inspector

```
                {
"bomFormat": "CycloneDX",
"specVersion": "1.4",
```

```
  "version": 1,
  "metadata": {
    "timestamp": "2023-06-02T01:17:46Z",
    "component": null,
    "properties": [
      {
        "name": "imageId",
        "value":
 "sha256:c8ee97f7052776ef223080741f61fcdf6a3a9107810ea9649f904aa4269fdac6"
      },
      {
        "name": "architecture",
        "value": "arm64"
      },
      {
        "name": "accountId",
        "value": "111122223333"
      },
      {
        "name": "resourceType",
        "value": "AWS_ECR_CONTAINER_IMAGE"
      }
    ]
  },
  "components": [
    {
      "type": "library",
      "name": "pip",
      "purl": "pkg:pypi/pip@22.0.4?path=usr/local/lib/python3.8/site-packages/
pip-22.0.4.dist-info/METADATA",
      "bom-ref": "98dc550d1e9a0b24161daaa0d535c699"
    },
    {
      "type": "application",
      "name": "libss2",
      "purl": "pkg:dpkg/libss2@1.44.5-1+deb10u3?
arch=ARM64&epoch=0&upstream=libss2-1.44.5-1+deb10u3.src.dpkg",
      "bom-ref": "2f4d199d4ef9e2ae639b4f8d04a813a2"
    },
    {
      "type": "application",
      "name": "liblz4-1",
      "purl": "pkg:dpkg/liblz4-1@1.8.3-1+deb10u1?
arch=ARM64&epoch=0&upstream=liblz4-1-1.8.3-1+deb10u1.src.dpkg",
```

```
      "bom-ref": "9a6be8907ead891b070e60f5a7b7aa9a"
    },
    {
      "type": "application",
      "name": "mawk",
      "purl": "pkg:dpkg/mawk@1.3.3-17+b3?
arch=ARM64&epoch=0&upstream=mawk-1.3.3-17+b3.src.dpkg",
      "bom-ref": "c2015852a729f97fde924e62a16f78a5"
    },
    {
      "type": "application",
      "name": "libgmp10",
      "purl": "pkg:dpkg/libgmp10@6.1.2+dfsg-4+deb10u1?
arch=ARM64&epoch=2&upstream=libgmp10-6.1.2+dfsg-4+deb10u1.src.dpkg",
      "bom-ref": "52907290f5beef00dff8da77901b1085"
    },
    {
      "type": "application",
      "name": "ncurses-bin",
      "purl": "pkg:dpkg/ncurses-bin@6.1+20181013-2+deb10u3?
arch=ARM64&epoch=0&upstream=ncurses-bin-6.1+20181013-2+deb10u3.src.dpkg",
      "bom-ref": "cd20cfb9ebeeadba3809764376f43bce"
    }
  ],
  "vulnerabilities": [
    {
      "id": "CVE-2022-40897",
      "affects": [
        {
          "ref": "a74a4862cc654a2520ec56da0c81cdb3"
        },
        {
          "ref": "0119eb286405d780dc437e7dbf2f9d9d"
        }
      ]
    }
  ]
}
```


Ejemplo del formato para SBOM de SPDX 2.3 de Amazon Inspector

```
{
 "name": "409870544328/EC2/i-022fba820db137c64/ami-074ea14c08effb2d8",
 "spdxVersion": "SPDX-2.3",
 "creationInfo": {
  "created": "2023-06-02T21:19:22Z",
  "creators": [
   "Organization: 409870544328",
   "Tool: Amazon Inspector SBOM Generator"
  ]
 },
 "documentNamespace": "EC2://i-022fba820db137c64/AMAZON_LINUX_2/null/x86_64",
 "comment": "",
 "packages": [{
   "name": "elfutils-libelf",
   "versionInfo": "0.176-2.amzn2",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
    "referenceCategory": "PACKAGE-MANAGER",
    "referenceType": "purl",
    "referenceLocator": "pkg:rpm/elfutils-libelf@0.176-2.amzn2?
arch=X86_64&epoch=0&upstream=elfutils-libelf-0.176-2.amzn2.src.rpm"
   }],
   "SPDXID": "SPDXRef-Package-rpm-elfutils-libelf-ddf56a513c0e76ab2ae3246d9a91c463"
  },
  {
   "name": "libcurl",
   "versionInfo": "7.79.1-1.amzn2.0.1",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
     "referenceCategory": "PACKAGE-MANAGER",
     "referenceType": "purl",
     "referenceLocator": "pkg:rpm/libcurl@7.79.1-1.amzn2.0.1?
arch=X86_64&epoch=0&upstream=libcurl-7.79.1-1.amzn2.0.1.src.rpm"
    },
    {
     "referenceCategory": "SECURITY",
     "referenceType": "vulnerability",
     "referenceLocator": "CVE-2022-32205"
    }
   ],
```

```
    "SPDXID": "SPDXRef-Package-rpm-libcurl-710fb33829bc5106559bcd380cddb7d5"
   },
   {
    "name": "hunspell-en-US",
    "versionInfo": "0.20121024-6.amzn2.0.1",
    "downloadLocation": "NOASSERTION",
    "sourceInfo": "/var/lib/rpm/Packages",
    "filesAnalyzed": false,
    "externalRefs": [{
     "referenceCategory": "PACKAGE-MANAGER",
     "referenceType": "purl",
     "referenceLocator": "pkg:rpm/hunspell-en-US@0.20121024-6.amzn2.0.1?
arch=NOARCH&epoch=0&upstream=hunspell-en-US-0.20121024-6.amzn2.0.1.src.rpm"
    }],
    "SPDXID": "SPDXRef-Package-rpm-hunspell-en-US-de19ae0883973d6cea5e7e079d544fe5"
   },
   {
    "name": "grub2-tools-minimal",
    "versionInfo": "2.06-2.amzn2.0.6",
    "downloadLocation": "NOASSERTION",
    "sourceInfo": "/var/lib/rpm/Packages",
    "filesAnalyzed": false,
    "externalRefs": [{
      "referenceCategory": "PACKAGE-MANAGER",
      "referenceType": "purl",
      "referenceLocator": "pkg:rpm/grub2-tools-minimal@2.06-2.amzn2.0.6?
arch=X86_64&epoch=1&upstream=grub2-tools-minimal-2.06-2.amzn2.0.6.src.rpm"
     },
     {
      "referenceCategory": "SECURITY",
      "referenceType": "vulnerability",
      "referenceLocator": "CVE-2021-3981"
     }
    ],
    "SPDXID": "SPDXRef-Package-rpm-grub2-tools-minimal-c56b7ea76e5a28ab8f232ef6d7564636"
   },
   {
    "name": "unixODBC-devel",
    "versionInfo": "2.3.1-14.amzn2",
    "downloadLocation": "NOASSERTION",
    "sourceInfo": "/var/lib/rpm/Packages",
    "filesAnalyzed": false,
    "externalRefs": [{
     "referenceCategory": "PACKAGE-MANAGER",
```

```
    "referenceType": "purl",
    "referenceLocator": "pkg:rpm/unixODBC-devel@2.3.1-14.amzn2?
arch=X86_64&epoch=0&upstream=unixODBC-devel-2.3.1-14.amzn2.src.rpm"
   }],
   "SPDXID": "SPDXRef-Package-rpm-unixODBC-devel-1bb35add92978df021a13fc9f81237d2"
  }
 ],
 "relationships": [{
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-elfutils-libelf-
ddf56a513c0e76ab2ae3246d9a91c463",
   "relationshipType": "DESCRIBES"
  },
  {
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-yajl-8476ce2db98b28cfab2b4484f84f1903",
   "relationshipType": "DESCRIBES"
  },
  {
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-unixODBC-
devel-1bb35add92978df021a13fc9f81237d2",
   "relationshipType": "DESCRIBES"
  }
 ],
 "SPDXID": "SPDXRef-DOCUMENT"
}
```


Filtros para SBOM

Al exportar SBOM, puede incluir filtros para crear informes de subconjuntos específicos de recursos. Si no proporciona un filtro, se exportarán las SBOM de todos los recursos activos y compatibles. Si, además, es administrador delegado, se incluirán los recursos de todos los miembros. Están disponibles los siguientes filtros:

- ID de cuenta: este filtro se utiliza para exportar SBOM de cualquier recurso asociado a un ID de cuenta específico.
- Etiqueta de instancia de EC2: este filtro se utiliza para exportar SBOM de instancias de EC2 con etiquetas específicas.

- Nombre de la función: este filtro se utiliza para exportar SBOM de funciones de Lambda específicas.
- Etiqueta de imagen: este filtro se utiliza para exportar SBOM de imágenes de contenedores con etiquetas específicas.
- Etiqueta de función de Lambda: este filtro se utiliza para exportar SBOM de funciones de Lambda con etiquetas específicas.
- Tipo de recurso: este filtro se utiliza para filtrar por tipo de recurso, que puede ser EC2, ECR o Lambda.
- ID de recurso: este filtro se utiliza para exportar una SBOM de un recurso específico.
- Nombre del repositorio: este filtro se utiliza para generar SBOM de imágenes de contenedores en repositorios específicos.

Configuración y exportación de SBOM

Para exportar SBOM, se requiere configurar antes un bucket de Amazon S3 y una clave de AWS KMS que Amazon Inspector pueda utilizar. Puede utilizar filtros para exportar SBOM de subconjuntos específicos de recursos. Para exportar SBOM de varias cuentas en una AWS Organization, siga estos pasos con la sesión iniciada como administrador delegado de Amazon Inspector.

Requisitos previos

- Recursos compatibles que se estén supervisando con Amazon Inspector.
- Un bucket de Amazon S3 configurado con una política que permite a Amazon Inspector agregar objetos al bucket. Para obtener información sobre cómo configurar la política, consulte Configuración de los permisos de exportación.
- Una clave de AWS KMS configurada con una política que permite a Amazon Inspector utilizarla para cifrar informes. Para obtener información sobre cómo configurar la política, consulte Configuración de una clave de AWS KMS de exportación.

> **Note**
>
> Si ya ha configurado un bucket de Amazon S3 y una clave de AWS KMS para exportar resultados, puede utilizar la misma combinación de bucket y clave para la exportación de SBOM.

Elija su método de acceso preferido para exportar una SBOM.

Console

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. En el selector de Región de AWS de la esquina superior derecha de la página, seleccione la región en la que se encuentran los recursos para los que desea exportar una SBOM.
3. En el panel de navegación, elija Exportar SBOM.
4. (Opcional) En la página Exportar SBOM, utilice el menú Agregar filtro para seleccionar el subconjunto de recursos para el que desea crear informes. Si no se proporciona ningún filtro, Amazon Inspector exportará informes de todos los recursos activos. Si es administrador delegado, se incluirán todos los recursos activos de la organización.
5. En Configuración de exportación, seleccione el formato de la SBOM.
6. Introduzca un URI de Amazon S3 o elija Explorar Amazon S3 para seleccionar la ubicación de Amazon S3 en la que desea almacenar la SBOM.
7. Introduzca la clave de AWS KMS configurada para Amazon Inspector que utilizará para cifrar los informes.

API

- Para exportar SBOM de recursos programáticamente, utilice la operación CreateSbomExport de la API de Amazon Inspector.

  En la solicitud, utilice el parámetro `reportFormat` para especificar el formato de salida de la SBOM, que puede ser `CYCLONEDX_1_4` o `SPDX_2_3`. Es obligatorio introducir el parámetro `s3Destination` y debe especificar un bucket de S3 configurado con una política que permita a Amazon Inspector escribir en él. Si lo desea, puede utilizar parámetros `resourceFilterCriteria` para limitar el alcance del informe a recursos específicos.

AWS CLI

- Para exportar las SBOM de sus recursos con la AWS Command Line Interface, ejecute el siguiente comando:

  ```
  aws inspector2 create-sbom-export --report-format
  FORMAT --s3-destination bucketName=DOC-EXAMPLE-
  BUCKET1,keyPrefix=PREFIX,kmsKeyArn=arn:aws:kms:Region:111122223333:key/123
  ```

En su solicitud, sustituya *FORMAT* por el formato que prefiera, `CYCLONEDX_1_4` o `SPDX_2_3`. A continuación, sustituya *user input placeholders* del destino de S3 por el nombre del bucket de S3 al que se vaya a exportar, el prefijo que se vaya a utilizar para la salida en S3 y el ARN de la clave de KMS que se vaya a utilizar para cifrar los informes.

Búsqueda en la base de datos de vulnerabilidades de Amazon Inspector

Puede buscar vulnerabilidades y exposiciones (CVE) en la base de datos de vulnerabilidades de Amazon Inspector. Amazon Inspector utiliza la información de la base de datos de vulnerabilidades para generar detalles relacionados con un ID de CVE. Puede acceder a estos detalles en una página de detalles del CVE.

En este tema se describe cómo buscar en la base de datos de vulnerabilidades de Amazon Inspector mediante un identificador de CVE e interpretar la página de detalles del CVE. Para obtener información sobre los resultados, consulte. Detalles de los hallazgos de Amazon Inspector

> **Note**
>
> Amazon Inspector rastrea y detecta otras vulnerabilidades de software en la base de datos. Sin embargo, Amazon Inspector solo admite los CVE con las plataformas que figuran en la sección Plataformas de detección de la página de detalles del CVE. Actualmente, la búsqueda en CVE no es compatible. Microsoft Windows

Buscando en la base de datos de vulnerabilidades

En esta sección se describe cómo buscar en la base de datos de vulnerabilidades en la consola y con la API de Amazon Inspector.

> **Note**
>
> Debe activar Amazon Inspector en su base de datos actual para Región de AWS poder buscar en la base de datos de vulnerabilidades.

Console

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/
2. En el panel de navegación, seleccione Búsqueda en la base de datos de vulnerabilidades.
3. En la barra de búsqueda, introduzca un ID de CVE y elija Buscar.

API

Ejecute la SearchVulnerabilitiesAPI de Amazon Inspector y proporcione un único ID de CVE con `filterCriteria` el siguiente formato:`CVE-<year>-<ID>`.

Comprenda los detalles del CVE

En esta sección se describe cómo interpretar la página de detalles del CVE.

Detalles del CVE

La sección de detalles del CVE incluye la siguiente información:

- Descripción e ID del CVE
- Gravedad de la CVE
- Puntuaciones del Common Vulnerability Scoring System (CVSS) y del Exploit Prediction Scoring System (EPSS)
- Plataformas de detección

> **Note**
>
> Si este campo está vacío, Amazon Inspector no admite la detección de tu ID de CVE.

- Enumeración de puntos débiles comunes (CWE)
- Fechas de creación y actualización del proveedor

Inteligencia sobre vulnerabilidades

La sección de inteligencia sobre vulnerabilidades proporciona datos de inteligencia sobre amenazas, como los objetivos de las vulnerabilidades y la última fecha de explotación pública conocida.

También proporciona datos de la Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA), que incluyen la acción correctiva, la fecha en que se agregó el CVE al catálogo de vulnerabilidades explotadas conocidas y la fecha en que la CISA espera que las agencias federales corrijan el CVE.

Referencias

La sección de referencias proporciona enlaces a recursos para obtener más información sobre el CVE.

Esquema de eventos de Amazon EventBridge para eventos de Amazon Inspector

Para facilitar la integración con otras aplicaciones, servicios y sistemas, incluidos sistemas de supervisión o administración de eventos, Amazon Inspector publica automáticamente los hallazgos en Amazon EventBridge como eventos. EventBridge es un servicio de bus de eventos sin servidor que ofrece una transmisión de datos en tiempo real desde aplicaciones y otros Servicios de AWS a distintos objetivos como funciones de AWS Lambda, temas de Amazon Simple Notification Service y transmisiones de Amazon Kinesis Data Streams. Para obtener más información acerca de EventBridge y los eventos de EventBridge, consulte la Guía del usuario de Amazon EventBridge.

Amazon Inspector publica eventos relacionados con hallazgos, cambios en la cobertura de los recursos y análisis iniciales de recursos. Cada evento es un objeto JSON que se adapta al esquema de EventBridge para los eventos de AWS. Como los datos están estructurados como un evento de EventBridge, los hallazgos y los eventos compatibles de Amazon Inspector son más fáciles de supervisar y procesar con otras aplicaciones, servicios y herramientas.

Temas

Esquema base de Amazon EventBridge para eventos de Amazon Inspector

A continuación se muestra un ejemplo del esquema básico de un evento de EventBridge para Amazon Inspector. Los detalles del evento varían según el tipo de evento.

```
{
    "version": "0",
    "id": "Event ID",
    "detail-type": "Inspector2 *event type*",
    "source": "aws.inspector2",
    "account": "Cuenta de AWS ID (string)",
    "time": "event timestamp (string)",
```

```
    "region": "Región de AWS (string)",
    "resources": [
        *IDs or ARNs of the resources involved in the event*
    ],
    "detail": {
        *Details of an Amazon Inspector event type*
    }
}
```

Ejemplo de esquema de eventos para hallazgos de Amazon Inspector

A continuación se muestra ejemplos del esquema de un evento de EventBridge para los hallazgos de Amazon Inspector. Los eventos de hallazgos se crean cuando Amazon Inspector identifica una vulnerabilidad de software o un problema de red en uno de sus recursos. Para leer la guía de creación de notificaciones en respuesta a este tipo de evento, consulte Creación de respuestas personalizadas para hallazgos de Amazon Inspector con Amazon EventBridge.

Los siguientes campos permiten identificar un evento de hallazgo:

- El campo `detail-type` se establece en `Inspector2 Finding`.
- El objeto `detail` describe el hallazgo.

Elija una de las siguientes opciones para consultar los esquemas de eventos de hallazgos para distintos recursos y tipos de hallazgo.

Amazon EC2 package vulnerability finding

```
{
    "version": "0",
    "id": "66a7a279-5f92-971c-6d3e-c92da0950992",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T22:46:15Z",
    "region": "us-east-1",
    "resources": ["i-0c2a343f1948d5205"],
    "detail": {
        "awsAccountId": "111122223333",
```

```
        "description": "\n It was discovered that the sound subsystem in the Linux
 kernel contained a\n race condition in some situations. A local attacker could use
 this to cause\n a denial of service (system crash).",
        "exploitAvailable": "YES",
        "exploitabilityDetails": {
            "lastKnownExploitAt": "Oct 24, 2022, 11:08:59 PM"
        },
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "fixAvailable": "YES",
        "lastObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "packageVulnerabilityDetails": {
            "cvss": [{
                "baseScore": 4.7,
                "scoringVector": "CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H",
                "source": "NVD",
                "version": "3.1"
            }],
            "referenceUrls": ["https://lore.kernel.org/all/
CAFcO6XN7JDM4xSXGhtusQfS2mSBcx50VJKwQpCq=WeLt57aaZA@mail.gmail.com/", "https://
ubuntu.com/security/notices/USN-5792-1", "https://ubuntu.com/security/notices/
USN-5791-2", "https://ubuntu.com/security/notices/USN-5791-1", "https://ubuntu.com/
security/notices/USN-5793-2", "https://git.kernel.org/pub/scm/linux/kernel/git/
torvalds/linux.git/commit/?id=8423f0b6d513b259fdab9c9bf4aaa6188d054c2d", "https://
ubuntu.com/security/notices/USN-5793-1", "https://ubuntu.com/security/notices/
USN-5792-2", "https://ubuntu.com/security/notices/USN-5791-3", "https://ubuntu.com/
security/notices/USN-5793-4", "https://ubuntu.com/security/notices/USN-5793-3",
 "https://git.kernel.org/linus/8423f0b6d513b259fdab9c9bf4aaa6188d054c2d(6.0-rc5)",
 "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3303"],
            "relatedVulnerabilities": [],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2022/
CVE-2022-3303.html",
            "vendorCreatedAt": "Sep 27, 2022, 11:15:00 PM",
            "vendorSeverity": "medium",
            "vulnerabilityId": "CVE-2022-3303",
            "vulnerablePackages": [{
                "arch": "X86_64",
                "epoch": 0,
                "fixedInVersion": "0:5.15.0.1027.31~20.04.16",
                "name": "linux-image-aws",
                "packageManager": "OS",
```

```
                "remediation": "apt update && apt install --only-upgrade linux-
image-aws",
                "version": "5.15.0.1026.30~20.04.16"
            }]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b7ff1a8d69f1bb35",
                    "ipV4Addresses": ["172.31.85.212", "44.203.45.27"],
                    "ipV6Addresses": [],
                    "launchedAt": "Jan 19, 2023, 7:53:14 PM",
                    "platform": "UBUNTU_20_04",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0c2a343f1948d5205",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "CVE-2022-3303 - linux-image-aws",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 10:46:15 PM"
    }
}
```


Amazon EC2 network reachability finding


```
{
```

```
    "version": "0",
    "id": "d0384f63-1621-1b75-d014-a5e45628ef3e",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T09:17:57Z",
    "region": "us-east-1",
    "resources": ["i-0a96278c2206a8e4b"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "On the instance i-0a96278c2206a8e4b, the port range
 22-22 is reachable from the InternetGateway igw-72069c09 from an attached ENI
 eni-0976efe678170408f.",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 20, 2023, 9:17:57 AM",
        "lastObservedAt": "Jan 20, 2023, 9:17:57 AM",
        "networkReachabilityDetails": {
            "networkPath": {
                "steps": [{
                    "componentId": "igw-72069c09",
                    "componentType": "AWS::EC2::InternetGateway"
                }, {
                    "componentId": "acl-91d74eec",
                    "componentType": "AWS::EC2::NetworkAcl"
                }, {
                    "componentId": "sg-0aaed0af450bd0165",
                    "componentType": "AWS::EC2::SecurityGroup"
                }, {
                    "componentId": "eni-0976efe678170408f",
                    "componentType": "AWS::EC2::NetworkInterface"
                }, {
                    "componentId": "i-0a96278c2206a8e4b",
                    "componentType": "AWS::EC2::Instance"
                }]
            },
            "openPortRange": {
                "begin": 22,
                "end": 22
            },
            "protocol": "TCP"
        },
        "remediation": {
            "recommendation": {
```

```
                "text": "You can restrict access to your instance by modifying the
 Security Groups or ACLs in the network path."
            }
        },
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b5eea76982371e91",
                    "ipV4Addresses": ["3.89.90.19", "172.31.93.57"],
                    "ipV6Addresses": [],
                    "keyName": "example-inspector-test",
                    "launchedAt": "Jan 19, 2023, 7:25:02 PM",
                    "platform": "AMAZON_LINUX_2",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0a96278c2206a8e4b",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "Port 22 is reachable from an Internet Gateway",
        "type": "NETWORK_REACHABILITY",
        "updatedAt": "Jan 20, 2023, 9:17:57 AM"
    }
}
```

Amazon ECR package vulnerability finding

```
{
    "version": "0",
    "id": "5b52952e-26df-3a51-6d14-4dbe737e58ec",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
```

```
    "time": "2023-01-19T21:59:00Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ecr:us-east-1:111122223333:repository/inspector2/
sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13"
    ],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "libcurl would reuse a previously created connection even
 when a TLS or SSHrelated option had been changed that should have prohibited
 reuse.libcurl keeps previously used connections in a connection pool for
 subsequenttransfers to reuse if one of them matches the setup. However, several TLS
 andSSH settings were left out from the configuration match checks, making themmatch
 too easily.",
        "exploitAvailable": "NO",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 9:59:00 PM",
        "fixAvailable": "YES",
        "inspectorScore": 7.5,
        "inspectorScoreDetails": {
            "adjustedCvss": {
                "adjustments": [],
                "cvssSource": "NVD",
                "score": 7.5,
                "scoreSource": "NVD",
                "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N",
                "version": "3.1"
            }
        },
        "lastObservedAt": "Jan 19, 2023, 9:59:00 PM",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 5,
                    "scoringVector": "AV:N/AC:L/Au:N/C:N/I:P/A:N",
                    "source": "NVD",
                    "version": "2.0"
                },
                {
                    "baseScore": 7.5,
                    "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N",
                    "source": "NVD",
                    "version": "3.1"
```

```
                }
            ],
            "referenceUrls": [
                "https://hackerone.com/reports/1555796",
                "https://security.gentoo.org/glsa/202212-01",
                "https://lists.debian.org/debian-lts-announce/2022/08/
msg00017.html",
                "https://www.debian.org/security/2022/dsa-5197"
            ],
            "relatedVulnerabilities": [],
            "source": "NVD",
            "sourceUrl": "https://nvd.nist.gov/vuln/detail/CVE-2022-27782",
            "vendorCreatedAt": "Jun 2, 2022, 2:15:00 PM",
            "vendorSeverity": "HIGH",
            "vendorUpdatedAt": "Jan 5, 2023, 5:51:00 PM",
            "vulnerabilityId": "CVE-2022-27782",
            "vulnerablePackages": [
                {
                    "arch": "X86_64",
                    "epoch": 0,
                    "fixedInVersion": "0:7.61.1-22.el8_6.3",
                    "name": "libcurl",
                    "packageManager": "OS",
                    "release": "22.el8",
                    "remediation": "yum update libcurl",
                    "sourceLayerHash":
 "sha256:38a980f2cc8accf69c23deae6743d42a87eb34a54f02396f3fcfd7c2d06e2c5b",
                    "version": "7.61.1"
                },
                {
                    "arch": "X86_64",
                    "epoch": 0,
                    "fixedInVersion": "0:7.61.1-22.el8_6.3",
                    "name": "curl",
                    "packageManager": "OS",
                    "release": "22.el8",
                    "remediation": "yum update curl",
                    "sourceLayerHash":
 "sha256:38a980f2cc8accf69c23deae6743d42a87eb34a54f02396f3fcfd7c2d06e2c5b",
                    "version": "7.61.1"
                }
            ]
        },
        "remediation": {
```

```
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [
            {
                "details": {
                    "awsEcrContainerImage": {
                        "architecture": "amd64",
                        "imageHash":
 "sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13",
                        "imageTags": [
                            "o3"
                        ],
                        "platform": "ORACLE_LINUX_8",
                        "pushedAt": "Jan 19, 2023, 7:38:39 PM",
                        "registry": "111122223333",
                        "repositoryName": "inspector2"
                    }
                },
                "id": "arn:aws:ecr:us-east-1:111122223333:repository/inspector2/
sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13",
                "partition": "aws",
                "region": "us-east-1",
                "type": "AWS_ECR_CONTAINER_IMAGE"
            }
        ],
        "severity": "HIGH",
        "status": "ACTIVE",
        "title": "CVE-2022-27782 - libcurl, curl",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 9:59:00 PM"
    }
}
```

Lambda package vulnerability finding

```
{
    "version": "0",
    "id": "040bb590-3a12-353f-ecb1-05e54b0fbea7",
    "detail-type": "Inspector2 Finding",
```

```
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T19:20:25Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:lambda:us-east-1:111122223333:function:ExampleFunction:$LATEST"
    ],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "Those using Woodstox to parse XML data may be vulnerable to
 Denial of Service attacks (DOS) if DTD support is enabled. If the parser is running
 on user supplied input, an attacker may supply content that causes the parser to
 crash by stackoverflow. This effect may support a denial of service attack.",
        "exploitAvailable": "NO",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 7:20:25 PM",
        "fixAvailable": "YES",
        "inspectorScore": 7.5,
        "inspectorScoreDetails": {
            "adjustedCvss": {
                "cvssSource": "NVD",
                "score": 7.5,
                "scoreSource": "NVD",
                "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
                "version": "3.1"
            }
        },
        "lastObservedAt": "Jan 19, 2023, 7:20:25 PM",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 7.5,
                    "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
                    "source": "NVD",
                    "version": "3.1"
                }
            ],
            "referenceUrls": [
                "https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47434"
            ],
            "relatedVulnerabilities": [],
            "source": "NVD",
            "sourceUrl": "https://nvd.nist.gov/vuln/detail/CVE-2022-40152",
```

```
            "vendorCreatedAt": "Sep 16, 2022, 10:15:00 AM",
            "vendorSeverity": "HIGH",
            "vendorUpdatedAt": "Nov 25, 2022, 11:15:00 AM",
            "vulnerabilityId": "CVE-2022-40152",
            "vulnerablePackages": [
                {
                    "epoch": 0,
                    "filePath": "lib/woodstox-core-6.2.7.jar",
                    "fixedInVersion": "6.4.0",
                    "name": "com.fasterxml.woodstox:woodstox-core",
                    "packageManager": "JAR",
                    "remediation": "Update woodstox-core to 6.4.0",
                    "version": "6.2.7"
                }
            ]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [
            {
                "details": {
                    "awsLambdaFunction": {
                        "architectures": [
                            "X86_64"
                        ],
                        "codeSha256": "+EwrOrht2um4fdVCD73gj
+O7HJIAUvUxi8AD0eKHSkc=",
                        "executionRoleArn": "arn:aws:iam::111122223333:role/
ExampleFunction-ExecutionRole",
                        "functionName": "Example-function",
                        "lastModifiedAt": "Nov 7, 2022, 8:29:27 PM",
                        "packageType": "ZIP",
                        "runtime": "JAVA_11",
                        "version": "$LATEST"
                    }
                },
                "id": "arn:aws:lambda:us-
east-1:111122223333:function:ExampleFunction:$LATEST",
                "partition": "aws",
                "region": "us-east-1",
                "tags": {
```

```
                    "TargetAlias": "DeploymentStack",
                    "SoftwareType": "Infrastructure"
                },
                "type": "AWS_LAMBDA_FUNCTION"
            }
        ],
        "severity": "HIGH",
        "status": "ACTIVE",
        "title": "CVE-2022-40152 - com.fasterxml.woodstox:woodstox-core",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 7:20:25 PM"
    }
}
```

Lambda code vulnerability finding

```
{
   "version":"0",
   "id":"9df01cb1-df24-bc46-5650-085a4087e7aa",
   "detail-type":"Inspector2 Finding",
   "source":"aws.inspector2",
   "account":"111122223333",
   "time":"2023-12-07T22:14:45Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:lambda:us-east-1:111122223333:function:code-finding:$LATEST"
   ],
   "detail":{
      "awsAccountId":"111122223333",
      "codeVulnerabilityDetails":{
         "detectorId":"python/lambda-override-reserved@v1.0",
         "detectorName":"Override of reserved variable names in a Lambda function",
         "detectorTags":[
            "availability",
            "aws-python-sdk",
            "aws-lambda",
            "data-integrity",
            "maintainability",
            "security",
            "security-context",
            "python"
```

```
         ],
         "filePath":{
            "endLine":6,
            "fileName":"lambda_function.py",
            "filePath":"lambda_function.py",
            "startLine":6
         },
         "ruleId":"Rule-434311"
      },
      "description":"Overriding environment variables that are reserved by AWS
 Lambda might lead to unexpected behavior or failure of the Lambda function.",
      "findingArn":"arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
      "firstObservedAt":"Aug 8, 2023, 7:33:58 PM",
      "lastObservedAt":"Dec 7, 2023, 10:14:45 PM",
      "remediation":{
         "recommendation":{
            "text":"Your code attempts to override an environment variable that is
 reserved by the Lambda runtime environment. This can lead to unexpected behavior
 and might break the execution of your Lambda function.\n\n[Learn more](https://
docs.aws.amazon.com/lambda/latest/dg/configuration-envvars.html#configuration-
envvars-runtime)"
         }
      },
      "resources":[
         {
            "details":{
               "awsLambdaFunction":{
                  "architectures":[
                     "X86_64"
                  ],
                  "codeSha256":"2mtfH+CgubesG6NYpb2zEqBja5WN6FfbH4AAYDuF8RE=",
                  "executionRoleArn":"arn:aws:iam::193043430472:role/service-role/
code-finding-role-7jgg3wan",
                  "functionName":"code-finding",
                  "lastModifiedAt":"Dec 7, 2023, 10:12:48 PM",
                  "packageType":"ZIP",
                  "runtime":"PYTHON_3_7",
                  "version":"$LATEST"
               }
            },
            "id":"arn:aws:lambda:us-east-1:193043430472:function:code-finding:
$LATEST",
            "partition":"aws",
            "region":"us-east-1",
```

```
            "type":"AWS_LAMBDA_FUNCTION"
         }
      ],
      "severity":"HIGH",
      "status":"ACTIVE",
      "title":"Overriding environment variables that are reserved by AWS Lambda
 might lead to unexpected behavior.",
      "type":"CODE_VULNERABILITY",
      "updatedAt":"Dec 7, 2023, 10:14:45 PM"
   }
}
```


> **Note**
>
> El valor del detalle devuelve los detalles del archivo JSON de un único hallazgo en forma de objeto. No devuelve la sintaxis de respuesta de todos los hallazgos, que admite varios hallazgos de una matriz.

Ejemplo de esquema de eventos completo para un análisis inicial de Amazon Inspector

A continuación se muestra un ejemplo del esquema de un evento de EventBridge para un evento de Amazon Inspector generado tras finalizar un análisis inicial. Este evento se crea cuando Amazon Inspector finaliza un análisis inicial de uno de sus recursos.

Los siguientes campos permiten identificar un evento finalizado para un análisis inicial:

- El campo `detail-type` se establece en `Inspector2 Scan`.
- El objeto `detail` contiene un objeto `finding-severity-counts` que describe detalladamente el número de hallazgos en las categorías de gravedad aplicables, incluidas `CRITICAL`, `HIGH` y `MEDIUM`.

Elija una de las siguientes opciones para consultar los distintos esquemas de eventos de análisis inicial por tipo de recurso.

Amazon EC2 instance initial scan


```
{
    "version": "0",
    "id": "28a46762-6ac8-6cc4-4f55-bc9ab99af928",
    "detail-type": "Inspector2 Scan",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T22:52:35Z",
    "region": "us-east-1",
    "resources": [
        "i-087d63509b8c97098"
    ],
    "detail": {
        "scan-status": "INITIAL_SCAN_COMPLETE",
        "finding-severity-counts": {
            "CRITICAL": 0,
            "HIGH": 0,
            "MEDIUM": 0,
            "TOTAL": 0
        },
        "instance-id": "i-087d63509b8c97098",
        "version": "1.0"
    }
}
```


Amazon ECR image initial scan


```
{
    "version": "0",
    "id": "fdaa751a-984c-a709-44f9-9a9da9cd3606",
    "detail-type": "Inspector2 Scan",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T23:15:18Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ecr:us-east-1:111122223333:repository/inspector2"
    ],
    "detail": {
```

```
        "scan-status": "INITIAL_SCAN_COMPLETE",
        "repository-name": "arn:aws:ecr:us-east-1:111122223333:repository/
inspector2",
        "finding-severity-counts": {
            "CRITICAL": 0,
            "HIGH": 0,
            "MEDIUM": 0,
            "TOTAL": 0
        },
        "image-digest":
 "sha256:965fbcae990b0467ed5657caceaec165018ef44a4d2d46c7cdea80a9dff0d1ea",
        "image-tags": [
            "ubuntu22"
        ],
        "version": "1.0"
    }
}
```

Lambda function initial scan

```
{
  "version": "0",
  "id": "4f290a7c-361b-c442-03c8-a629f6f20d6c",
  "detail-type": "Inspector2 Scan",
  "source": "aws.inspector2",
  "account": "111122223333",
  "time": "2023-02-23T18:06:03Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:lambda:us-west-2:111122223333:function:lambda-example:$LATEST"
  ],
  "detail": {
    "scan-status": "INITIAL_SCAN_COMPLETE",
    "finding-severity-counts": {
      "CRITICAL": 0,
      "HIGH": 0,
      "MEDIUM": 0,
      "TOTAL": 0
    },
    "version": "1.0"
```

```
  }
}
```

Ejemplo de esquema de eventos de cobertura de Amazon Inspector

A continuación se muestra un ejemplo del esquema de un evento de EventBridge para un evento de cobertura de Amazon Inspector. Este evento se crea cuando se modifica la cobertura de análisis de Amazon Inspector de un recurso. Los siguientes campos permiten identificar un evento de cobertura:

- El campo `detail-type` se establece en `Inspector2 Coverage`.
- El objeto `detail` contiene un objeto `scanStatus` que indica el nuevo estado de análisis del recurso.

```
{
    "version": "0",
    "id": "000adda5-0fbf-913e-bc0e-10f0376412aa",
    "detail-type": "Inspector2 Coverage",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T22:51:39Z",
    "region": "us-east-1",
    "resources": [
        "i-087d63509b8c97098"
    ],
    "detail": {
        "scanStatus": {
            "reason": "UNMANAGED_EC2_INSTANCE",
            "statusCodeValue": "INACTIVE"
        },
        "scanType": "PACKAGE",
        "eventTimestamp": "2023-01-20T22:51:35.665501Z",
        "version": "1.0"
    }
}
```

Integración de análisis de Amazon Inspector en su canalización de CI/CD

Puede integrar los análisis de imágenes de contenedores de Amazon Inspector directamente en su canalización de CI/CD para detectar vulnerabilidades de software y proporcionar informes al final de la compilación. Los informes de vulnerabilidades generados por Amazon Inspector le permiten investigar y corregir los riesgos antes de la implementación.

La integración de CI/CD de Amazon Inspector utiliza una combinación del Generador de SBOM de Amazon Inspector y la API de Amazon Inspector Scan para generar informes de vulnerabilidad para las imágenes de sus contenedores. El Generador de SBOM de Amazon Inspector crea una lista de materiales de software (SBOM) a partir de una imagen de contenedor proporcionada y, a continuación, la API de Amazon Inspector Scan analiza esa SBOM y crea un informe con detalles sobre las vulnerabilidades detectadas.

Puede lograr una integración de CI/CD con Amazon Inspector mediante los complementos de Amazon Inspector diseñados específicamente para soluciones de CI/CD individuales y disponibles en su mercado, o puede crear su propia integración de análisis personalizada.

Temas

Integración de complementos

Amazon Inspector proporciona complementos para las soluciones de CI/CD compatibles. Puede instalar estos complementos desde sus respectivos mercados y luego usarlos para añadir análisis

de Amazon Inspector como paso de generación en su canalización. El paso de creación de complementos ejecuta el Generador de SBOM de Amazon Inspector en la imagen que proporcione y, a continuación, ejecuta la API de Amazon Inspector Scan en la SBOM generada.

La siguiente es una descripción general de cómo funciona la integración de CI/CD de Amazon Inspector a través de complementos:

1. Debe configurar y permitir Cuenta de AWS el acceso a la API de escaneo de Amazon Inspector. Para ver instrucciones, consulte Configuración de una AWS cuenta para usar la integración CI/CD de Amazon Inspector.
2. El complemento Amazon Inspector se instala desde el mercado.
3. Debe instalar y configurar el binario del Generador de SBOM de Amazon Inspector. Para ver instrucciones, consulte Generador SBOM de Amazon Inspector.
4. Añada Amazon Inspector Scans como paso de compilación en su proceso de CI/CD y configure el análisis.
5. Cuando ejecuta una compilación, el complemento toma la imagen del contenedor como entrada y, a continuación, ejecuta el Generador de SBOM de Amazon Inspector en la imagen para generar una SBOM compatible con CycloneDX.
6. Desde allí, el complemento envía la SBOM generada a un punto de conexión de la API de Amazon Inspector Scan, que evalúa cada componente de la SBOM en busca de vulnerabilidades.
7. La respuesta de la API de Amazon Inspector Scan se transforma en un informe de vulnerabilidades en los formatos CSV, SBOM, JSON y HTML. El informe contiene detalles sobre las vulnerabilidades que haya encontrado Amazon Inspector.

Soluciones de CI/CD compatibles

Amazon Inspector admite actualmente las siguientes soluciones de CI/CD. Para obtener instrucciones completas sobre cómo configurar la integración de CI/CD mediante un complemento, seleccione el complemento para su solución de CI/CD:

- Complemento Jenkins
- Complemento de TeamCity

Integración personalizada

Si Amazon Inspector no proporciona complementos para su solución de CI/CD, puede crear su propia integración de CI/CD personalizada mediante una combinación del Generador de SBOM de Amazon Inspector y la API de Amazon Inspector Scan. También puede utilizar una integración personalizada para ajustar los análisis con las opciones disponibles a través del Generador de SBOM de Amazon Inspector.

La siguiente es una descripción general de cómo funciona la integración de CI/CD de Amazon Inspector:

1. Debe configurar y permitir Cuenta de AWS el acceso a la API de escaneo de Amazon Inspector. Para ver instrucciones, consulte Configuración de una AWS cuenta para usar la integración CI/CD de Amazon Inspector.
2. Debe instalar y configurar el binario del Generador de SBOM de Amazon Inspector. Para ver instrucciones, consulte Generador SBOM de Amazon Inspector.
3. Utilice el Generador de SBOM de Amazon Inspector para generar una SBOM compatible con CycloneDX para la imagen de su contenedor.
4. Utilice la API de Amazon Inspector Scan en la SBOM generada para generar un informe de vulnerabilidades.

Para obtener instrucciones sobre cómo configurar una integración personalizada, consulte Creación de su propia integración personalizada de canalizaciones de CI/CD con Amazon Inspector Scan.

Configuración de una AWS cuenta para usar la integración CI/CD de Amazon Inspector

Debe registrarse y utilizar la integración Cuenta de AWS CI/CD de Amazon Inspector. Cuenta de AWS Debe tener una función de IAM que conceda a tu canalización acceso a la API de escaneo de Amazon Inspector.

Complete las tareas de los siguientes temas para suscribirse a un rol de IAM Cuenta de AWS, crear un usuario administrador y configurar un rol de IAM para la integración de CI/CD.

> **Note**
>
> Si ya se ha registrado para obtener un Cuenta de AWS, puede pasar a. Configuración de un rol de IAM para la integración de CI/CD

Temas

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario administrativo y utilice únicamente el usuario raíz para ejecutar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento en https://aws.amazon.com/ y en Mi cuenta.

Cómo crear un usuario administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda sobre cómo iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Cómo crear un usuario administrativo

1. Activar IAM Identity Center

   Consulte las instrucciones en Enabling AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En el Centro de identidades de IAM, conceda acceso administrativo a un usuario administrativo.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario administrativo

- Para iniciar sesión con el usuario del IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario del Centro de identidades de IAM.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Configuración de un rol de IAM para la integración de CI/CD

Para integrar el análisis de Amazon Inspector en su canalización de CI/CD, debe crear una política de IAM que permita el acceso a la API de Amazon Inspector Scan, que analiza la lista de materiales

de software (SBOM). A continuación, puede adjuntar esa política a un rol de IAM que su cuenta pueda asumir para ejecutar la API de Amazon Inspector Scan.

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la consola de IAM, elija Políticas y, a continuación, Crear política.
3. En Editor de políticas, seleccione JSON y pegue la declaración instrucción:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "inspector-scan:ScanSbom",
            "Resource": "*"
        }
    ]
}
```

4. Elija Siguiente.
5. Introduzca un nombre para la política, por ejemplo `InspectorCICDscan-policy`, y una descripción, y a continuación elija Crear política. Esta política se adjuntará al rol que va a crear en los pasos siguientes.
6. En el panel de navegación de la consola de IAM, elija Roles y, a continuación, Crear nuevo rol.
7. En Tipo de entidad de confianza, seleccione Política de confianza personalizada y, a continuación, introduzca la siguiente política:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{ACCOUNT_ID}:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
```

```
        }
    ]
}
```

8. Elija Siguiente.
9. En la página Agregar permisos, busque y seleccione la política que creó anteriormente y, a continuación, seleccione Siguiente.
10. Introduzca un nombre para el rol, por ejemplo `InspectorCICDscan-role`, y una descripción, y a continuación elija `Create Role`.

Generador SBOM de Amazon Inspector

El Generador SBOM de Amazon Inspector (Sbomgen) es una herramienta binaria que genera una lista de materiales de software (SBOM) para una imagen de contenedor. Una SBOM es un inventario que recopila el software instalado en un sistema.

Sbomgen busca los archivos que se sabe que contienen información sobre los paquetes instalados. Si encuentra alguno de estos archivos, la herramienta extrae los nombres, las versiones y otros metadatos de los paquetes. A continuación, los metadatos de este paquete se transforman en una SBOM de CycloneDX .

Sbomgen se puede utilizar como herramienta independiente para proporcionar la SBOM de CycloneDX en forma de archivo o en formato STDOUT. También se utiliza como parte de la integración de CI/CD de Amazon Inspector, que escanea automáticamente las imágenes de los contenedores como parte del proceso de implementación. Para obtener más información, consulte Integración de análisis de Amazon Inspector en su canalización de CI/CD.

Paquetes y formatos de imagen compatibles

En este momento, Sbomgen puede recopilar el inventario de los siguientes tipos de paquetes:

- Alpine APK
- Debian / Ubuntu DPKG
- Red Hat RPM
- Paquetes Go a través de `go.mod` y `go mod cache`
- Paquetes Java a través de `pom.properties`

- Paquetes Node.js a través de archivos `package.json` dentro de `node_modules`
- Paquetes C# a través de archivos Nuget (`.deps.json`, `csproj`, `Packages.config`, packages.lock.json)
- PHP a través de `installed.json` y `composer.lock`
- Paquetes Python a través de archivos `requirements.txt`, `Pipfile.lock`, `poetry.lock` y `egg/wheel`
- Paquetes Ruby a través de `Gemfile.lock`, `.gemspec` y gemas instaladas globalmente
- Paquetes Rust a través de `Cargo.lock` y `Cargo.toml`

Sbomgen admite los siguientes formatos del manifiesto de imágenes de contenedor para la imágenes:

- Manifiesto de imágenes de OCI
- Manifiesto de imágenes de Docker versión 2, esquema 2
- Manifiesto de imágenes de Docker versión 2, esquema 1
- Manifiesto de imágenes de Docker versión 1

> **Important**
>
> Sbomgen no puede escanear las imágenes del contenedor si tienen un tamaño superior a 5 GB, más de 60 capas o más de 2000 paquetes instalados.

Instalación del Generador de SBOM de Amazon Inspector (Sbomgen)

Sbomgen solo está disponible para los sistemas operativos Linux. Si lo utiliza para analizar imágenes de contenedores, debe tener instalado un servicio de contenedores, como Docker, Podman o containerd.

Para obtener el mejor rendimiento, se recomienda ejecutar el binario desde un sistema con estas especificaciones de hardware mínimas:

- CPU de 4 núcleos
- 8 GB de RAM

Para instalar Sbomgen

1. Descargue el archivo zip de Sbomgen desde la URL correcta para su arquitectura:

   Linux AMD64:

   https://amazon-inspector-sbomgen.s3.amazonaws.com/latest/linux/amd64/inspector-sbomgen.zip

   Linux ARM64:

   https://amazon-inspector-sbomgen.s3.amazonaws.com/latest/linux/arm64/inspector-sbomgen.zip
2. Descomprima el archivo descargado con el siguiente comando:

   ```
   unzip inspector-sbomgen.zip
   ```
3. Compruebe si hay los siguientes archivos en el archivo:

   - `inspector-sbomgen`: el binario que ejecutará para generar las SBOM.
   - `README.txt`: la documentación para usar Sbomgen.
   - `LICENSE.txt`: archivo que contiene la licencia de software de Sbomgen.
   - `licenses`: carpeta que contiene información de licencia de los paquetes de terceros utilizados por Sbomgen.
   - `checksums.txt`: archivo que proporciona los hashes del binario de Sbomgen.
   - `sbom.json`: una SBOM de CycloneDX para el binario de Sbomgen.
4. (Opcional) Verifique la autenticidad y la integridad del binario mediante el siguiente comando:

   ```
   sha256sum < inspector-sbomgen
   ```

   - Compare los resultados con el contenido del archivo `checksums.txt`.
5. Otorgue los permisos ejecutables mediante el siguiente comando.

   ```
   chmod +x inspector-sbomgen
   ```
6. Con los siguientes comandos, verifique si Sbomgen se ha instalado correctamente:

   ```
   ./inspector-sbomgen --version
   ```

   Debería ver un resultado similar a este:

```
Version: 1.X.X
```

Uso de Sbomgen

Sbomgen se puede utilizar para generar una SBOM para imágenes de contenedores.

También puede personalizar los resultados de la generación de la SBOM mediante varias opciones. Por ejemplo, puede excluir archivos específicos o definir que paquetes busca la herramienta. Para ver ejemplos de estos y otros casos de uso, ejecute el siguiente comando:

```
./inspector-sbomgen list-examples
```

Para generar una SBOM para una imagen de contenedor y enviar el resultado a un archivo

Para este ejemplo, sustituya *image:tag* por el ID de la imagen y *output_path.json* por la ruta en la que se vaya a guardar el resultado:

```
./inspector-sbomgen container --image image:tag -o output_path.json
```

Autenticación en registros privados con Sbomgen

Para generar una SBOM a partir de sus contenedores alojados en registros privados, puede proporcionar sus credenciales de autenticación de registro privado. Puede proporcionar sus credenciales de varias formas: mediante credenciales en caché, mediante un método interactivo o con un método no interactivo en el que las credenciales se proporcionen como variables de entorno antes de ejecutar Sbomgen.

Autenticación mediante credenciales almacenadas en caché (recomendado)

1. Sbomgen intentará utilizar las credenciales almacenadas en caché si están disponibles en su agente. Para este método, autentifíquese primero en el registro de su contenedor. Por ejemplo, si utiliza Docker, puede autenticarse en su registro mediante el comando `login` de Docker:

   ```
   docker login
   ```
2. A continuación, tras autenticarse correctamente en su registro privado, puede usar Sbomgen en una imagen de contenedor de ese registro. Para usar el ejemplo siguiente, sustituya *image:tag* por el nombre de la imagen que se vaya a escanear:

   ```
   ./inspector-sbomgen container --image image:tag
   ```

Autenticación mediante el método interactivo

- Para este método, proporcione su nombre de usuario como parámetro y Sbomgen le solicitará que introduzca la contraseña de forma segura cuando sea necesario. Para usar el ejemplo siguiente, sustituya *image:tag* por el nombre de la imagen que se vaya a escanear y *your_username* por un nombre de usuario que tenga acceso a esa imagen:

  ```
  ./inspector-sbomgen container --image image:tag --username
  your_username
  ```

Autenticación mediante el método no interactivo

- Para utilizar este método, debe almacenar la contraseña o el token de registro en un archivo .txt que solo pueda leer el usuario actual. El archivo de texto debe contener únicamente la contraseña o el token en una sola línea. Para usar el ejemplo siguiente, sustituya *your_username* por su nombre de usuario, *password.txt* por el archivo que contenga su contraseña o token y *image:tag* por el nombre de la imagen que desee escanear:

  ```
  INSPECTOR_SBOMGEN_USERNAME=your_username\
  INSPECTOR_SBOMGEN_PASSWORD=`cat password.txt` \
  ./inspector-sbomgen container --image image:tag
  ```

Ejemplos de resultados de Sbomgen

A continuación se muestra un ejemplo de una SBOM de una imagen de contenedor inventariada que utiliza Sbomgen.

SBOM de imagen de contenedor


```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.5",
  "serialNumber": "urn:uuid:828875ef-8c32-4777-b688-0af96f3cf619",
  "version": 1,
  "metadata": {
    "timestamp": "2023-11-17T21:36:38Z",
    "tools": [
      {
        "vendor": "Amazon Web Services, Inc. (AWS)",
```

```
        "name": "Amazon Inspector SBOM Generator",
        "version": "1.0.0",
        "hashes": [
          {
            "alg": "SHA-256",
            "content":
"10ab669cfc99774786301a745165b5957c92ed9562d19972fbf344d4393b5eb1"
          }
        ]
      }
    ],
    "component": {
      "bom-ref": "comp-1",
      "type": "container",
      "name": "fedora:latest",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:image_id",
          "value":
"sha256:c81c8ae4dda7dedc0711daefe4076d33a88a69a28c398688090c1141eff17e50"
        },
        {
          "name": "amazon:inspector:sbom_generator:layer_diff_id",
          "value":
"sha256:eddd0d48c295dc168d0710f70364581bd84b1dda6bb386c4a4de0b61de2f2119"
        }
      ]
    }
  },
  "components": [
    {
      "bom-ref": "comp-2",
      "type": "library",
      "name": "dnf",
      "version": "4.18.0",
      "purl": "pkg:pypi/dnf@4.18.0",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:source_file_scanner",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_package_collector",
          "value": "python-pkg"
```

```
        },
        {
          "name": "amazon:inspector:sbom_generator:source_path",
          "value": "/usr/lib/python3.12/site-packages/dnf-4.18.0.dist-info/METADATA"
        },
        {
          "name": "amazon:inspector:sbom_generator:is_duplicate_package",
          "value": "true"
        },
        {
          "name": "amazon:inspector:sbom_generator:duplicate_purl",
          "value": "pkg:rpm/fedora/python3-dnf@4.18.0-2.fc39?
arch=noarch&distro=39&epoch=0"
        }
      ]
    },
    {
      "bom-ref": "comp-3",
      "type": "library",
      "name": "libcomps",
      "version": "0.1.20",
      "purl": "pkg:pypi/libcomps@0.1.20",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:source_file_scanner",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_package_collector",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_path",
          "value": "/usr/lib64/python3.12/site-packages/libcomps-0.1.20-py3.12.egg-
info/PKG-INFO"
        },
        {
          "name": "amazon:inspector:sbom_generator:is_duplicate_package",
          "value": "true"
        },
        {
          "name": "amazon:inspector:sbom_generator:duplicate_purl",
          "value": "pkg:rpm/fedora/python3-libcomps@0.1.20-1.fc39?
arch=x86_64&distro=39&epoch=0"
```

```
        }
      ]
    }
  ]
}
```

Creación de su propia integración personalizada de canalizaciones de CI/CD con Amazon Inspector Scan

Recomendamos utilizar los complementos de CI/CD de Amazon Inspector si están disponibles en la tienda de CI/CD. Para ver una lista de los complementos disponibles, consulte Soluciones de CI/CD compatibles.

Si Amazon Inspector no proporciona complementos para su solución de CI/CD, puede crear su propia integración de CI/CD personalizada mediante una combinación del Generador de SBOM de Amazon Inspector y la API de Amazon Inspector Scan. También puede utilizar una integración personalizada para ajustar los análisis mediante las opciones disponibles en el Generador de SBOM de Amazon Inspector.

Para configurar su propia integración personalizada

1. Configure y Cuenta de AWS permita el acceso a la API de escaneo de Amazon Inspector. Para ver instrucciones, consulte Configuración de una AWS cuenta para usar la integración CI/CD de Amazon Inspector.
2. Instale y configure el binario del Generador de SBOM de Amazon Inspector. Para ver instrucciones, consulte Instalación del Generador de SBOM de Amazon Inspector (Sbomgen).
3. Utilice el generador de SBOM para crear un archivo SBOM para la imagen del contenedor que desee analizar. Para usar el ejemplo siguiente, sustituya *image:id* por el nombre de la imagen que se vaya a analizar y *sbom_path.json* por la ubicación en la que se vaya guardar el resultado de la SBOM:

   ```
   ./inspector-sbomgen container –image image:id -o sbom_path.json
   ```

4. Llame a la API de `inspector-scan` para analizar la SBOM generada y proporcionar un informe de vulnerabilidades. Para usar el siguiente ejemplo, sustituya *sbom_path.json* por la ruta de un archivo de SBOM válido y compatible con CyclonedX. A continuación, sustituya *ENDPOINT* por el punto final de la API en el Región de AWS que está autenticado actualmente y

sustituya *REGION* por la región correspondiente. Para obtener una lista completa de regiones y puntos de conexión, consulte Puntos de conexión para la API de Amazon Inspector Scan.

```
aws inspector-scan scan-sbom --sbom file://sbom_path.json --endpoint
"ENDPOINT" --region REGION
```

Formatos de resultados de la API

La API de Amazon Inspector Scan puede generar un informe de vulnerabilidades en formato CycloneDX 1.5 o resultados de JSON de Amazon Inspector. El valor predeterminado se puede cambiar con la marca `--output-format`.

Ejemplo de resultado en formato CycloneDX 1.5


```
{
  "status": "SBOM parsed successfully, 1 vulnerabilities found",
  "sbom": {
    "bomFormat": "CycloneDX",
    "specVersion": "1.5",
    "serialNumber": "urn:uuid:0077b45b-ff1e-4dbb-8950-ded11d8242b1",
    "metadata": {
      "properties": [
        {
          "name": "amazon:inspector:sbom_scanner:critical_vulnerabilities",
          "value": "1"
        },
        {
          "name": "amazon:inspector:sbom_scanner:high_vulnerabilities",
          "value": "0"
        },
        {
          "name": "amazon:inspector:sbom_scanner:medium_vulnerabilities",
          "value": "0"
        },
        {
          "name": "amazon:inspector:sbom_scanner:low_vulnerabilities",
          "value": "0"
        }
      ],
      "tools": [
        {
          "name": "CycloneDX SBOM API",
```

```
          "vendor": "Amazon Inspector",
          "version": "empty:083c9b00:083c9b00:083c9b00"
        }
      ],
      "timestamp": "2023-06-28T14:15:53.760Z"
    },
    "components": [
      {
        "bom-ref": "comp-1",
        "type": "library",
        "name": "log4j-core",
        "purl": "pkg:maven/org.apache.logging.log4j/log4j-core@2.12.1",
        "properties": [
          {
            "name": "amazon:inspector:sbom_scanner:path",
            "value": "/home/dev/foo.jar"
          }
        ]
      }
    ],
    "vulnerabilities": [
      {
        "bom-ref": "vuln-1",
        "id": "CVE-2021-44228",
        "source": {
          "name": "NVD",
          "url": "https://nvd.nist.gov/vuln/detail/CVE-2021-44228"
        },
        "references": [
          {
            "id": "SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720",
            "source": {
              "name": "SNYK",
              "url": "https://security.snyk.io/vuln/SNYK-JAVA-
ORGAPACHELOGGINGLOG4J-2314720"
            }
          },
          {
            "id": "GHSA-jfh8-c2jp-5v3q",
            "source": {
              "name": "GITHUB",
              "url": "https://github.com/advisories/GHSA-jfh8-c2jp-5v3q"
            }
          }
```

```
        ],
        "ratings": [
          {
            "source": {
              "name": "NVD",
              "url": "https://www.first.org/cvss/v3-1/"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
          },
          {
            "source": {
              "name": "NVD",
              "url": "https://www.first.org/cvss/v2/"
            },
            "score": 9.3,
            "severity": "critical",
            "method": "CVSSv2",
            "vector": "AC:M/Au:N/C:C/I:C/A:C"
          },
          {
            "source": {
              "name": "EPSS",
              "url": "https://www.first.org/epss/"
            },
            "score": 0.97565,
            "severity": "none",
            "method": "other",
            "vector": "model:v2023.03.01,date:2023-06-27T00:00:00+0000"
          },
          {
            "source": {
              "name": "SNYK",
              "url": "https://security.snyk.io/vuln/SNYK-JAVA-
ORGAPACHELOGGINGLOG4J-2314720"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H"
          },
          {
```

```
            "source": {
              "name": "GITHUB",
              "url": "https://github.com/advisories/GHSA-jfh8-c2jp-5v3q"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
          }
        ],
        "cwes": [
          400,
          20,
          502
        ],
        "description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security
 releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages,
 and parameters do not protect against attacker controlled LDAP and other JNDI related
 endpoints. An attacker who can control log messages or log message parameters can
 execute arbitrary code loaded from LDAP servers when message lookup substitution is
 enabled. From log4j 2.15.0, this behavior has been disabled by default. From version
 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely
 removed. Note that this vulnerability is specific to log4j-core and does not affect
 log4net, log4cxx, or other Apache Logging Services projects.",
        "advisories": [
          {
            "url": "https://www.intel.com/content/www/us/en/security-center/advisory/
intel-sa-00646.html"
          },
          {
            "url": "https://support.apple.com/kb/HT213189"
          },
          {
            "url": "https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-
cve-2021-44228-apache-log4j2/"
          },
          {
            "url": "https://logging.apache.org/log4j/2.x/security.html"
          },
          {
            "url": "https://www.debian.org/security/2021/dsa-5020"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf"
```

```
          },
          {
            "url": "https://www.oracle.com/security-alerts/alert-cve-2021-44228.html"
          },
          {
            "url": "https://www.oracle.com/security-alerts/cpujan2022.html"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf"
          },
          {
            "url": "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/M5CSVUNV4HWZZXGOKNSK6L7RPM7BOKIB/"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf"
          },
          {
            "url": "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/VU57UJDCFIASIO35GC55JMKSRXJMCDFM/"
          },
          {
            "url": "https://www.oracle.com/security-alerts/cpuapr2022.html"
          },
          {
            "url": "https://twitter.com/kurtseifried/status/1469345530182455296"
          },
          {
            "url": "https://tools.cisco.com/security/center/content/
CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd"
          },
          {
            "url": "https://lists.debian.org/debian-lts-announce/2021/12/msg00007.html"
          },
          {
            "url": "https://www.kb.cert.org/vuls/id/930724"
          }
        ],
        "created": "2021-12-10T10:15:00Z",
        "updated": "2023-04-03T20:15:00Z",
        "affects": [
```

```
          {
            "ref": "comp-1"
          }
        ],
        "properties": [
          {
            "name": "amazon:inspector:sbom_scanner:exploit_available",
            "value": "true"
          },
          {
            "name": "amazon:inspector:sbom_scanner:exploit_last_seen_in_public",
            "value": "2023-03-06T00:00:00Z"
          },
          {
            "name": "amazon:inspector:sbom_scanner:cisa_kev_date_added",
            "value": "2021-12-10T00:00:00Z"
          },
          {
            "name": "amazon:inspector:sbom_scanner:cisa_kev_date_due",
            "value": "2021-12-24T00:00:00Z"
          },
          {
            "name": "amazon:inspector:sbom_scanner:fixed_version:comp-1",
            "value": "2.15.0"
          }
        ]
      }
    ]
  }
}
```

Ejemplo de resultado en formato Inspector

```
                        {
  "status": "SBOM parsed successfully, 1 vulnerability found",
  "inspector": {
    "messages": [
      {
        "name": "foo",
        "purl": "pkg:maven/foo@1.0.0", // Will not exist in output if missing in sbom
        "info": "Component skipped: no rules found."
      }
```

```
    ],
    "vulnerability_count": {
      "critical": 1,
      "high": 0,
      "medium": 0,
      "low": 0
    },
    "vulnerabilities": [
      {
        "id": "CVE-2021-44228",
        "severity": "critical",
        "source": "https://nvd.nist.gov/vuln/detail/CVE-2021-44228",
        "related": [
          "SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720",
          "GHSA-jfh8-c2jp-5v3q"
        ],
        "description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security
 releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages,
 and parameters do not protect against attacker controlled LDAP and other JNDI related
 endpoints. An attacker who can control log messages or log message parameters can
 execute arbitrary code loaded from LDAP servers when message lookup substitution is
 enabled. From log4j 2.15.0, this behavior has been disabled by default. From version
 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely
 removed. Note that this vulnerability is specific to log4j-core and does not affect
 log4net, log4cxx, or other Apache Logging Services projects.",
        "references": [
          "https://www.intel.com/content/www/us/en/security-center/advisory/intel-
sa-00646.html",
          "https://support.apple.com/kb/HT213189",
          "https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-
cve-2021-44228-apache-log4j2/",
          "https://logging.apache.org/log4j/2.x/security.html",
          "https://www.debian.org/security/2021/dsa-5020",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf",
          "https://www.oracle.com/security-alerts/alert-cve-2021-44228.html",
          "https://www.oracle.com/security-alerts/cpujan2022.html",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf",
          "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/M5CSVUNV4HWZZXGOKNSK6L7RPM7BOKIB/",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf",
          "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/VU57UJDCFIASIO35GC55JMKSRXJMCDFM/",
          "https://www.oracle.com/security-alerts/cpuapr2022.html",
```

```
          "https://twitter.com/kurtseifried/status/1469345530182455296",
          "https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-
sa-apache-log4j-qRuKNEbd",
          "https://lists.debian.org/debian-lts-announce/2021/12/msg00007.html",
          "https://www.kb.cert.org/vuls/id/930724"
        ],
        "created": "2021-12-10T10:15:00Z",
        "updated": "2023-04-03T20:15:00Z",
        "properties": {
          "cisa_kev_date_added": "2021-12-10T00:00:00Z",
          "cisa_kev_date_due": "2021-12-24T00:00:00Z",
          "cwes": [
            400,
            20,
            502
          ],
          "cvss": [
            {
              "source": "NVD",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H",
              "cvss2_base_score": 9.3,
              "cvss2_base_vector": "AC:M/Au:N/C:C/I:C/A:C"
            },
            {
              "source": "SNYK",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H"
            },
            {
              "source": "GITHUB",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
            }
          ],
          "epss": 0.97565,
          "exploit_available": true,
          "exploit_last_seen_in_public": "2023-03-06T00:00:00Z"
        },
        "affects": [
          {
```

```
            "installed_version": "pkg:maven/org.apache.logging.log4j/log4j-
core@2.12.1",
            "fixed_version": "2.15.0",
            "path": "/home/dev/foo.jar"
          }
        ]
      }
    ]
  }
}
```

Uso del complemento Jenkins de Amazon Inspector

El Jenkins complemento aprovecha el binario Amazon Inspector SBOM Generator y la API Amazon Inspector Scan para generar informes detallados al final de la compilación, de modo que pueda investigar y corregir el riesgo antes de la implementación.

Amazon Inspector es un servicio de gestión de vulnerabilidades que escanea las imágenes de los contenedores en busca de vulnerabilidades de paquetes de sistemas operativos y lenguajes de programación basadas en CVE.

Con el Jenkins complemento Amazon Inspector, puede añadir escaneos de vulnerabilidades de Amazon Inspector a su Jenkins proceso.

> **Note**
>
> Los escaneos de vulnerabilidades de Amazon Inspector se pueden configurar para que aprueben o rechacen las ejecuciones de canalización en función del número y la gravedad de las vulnerabilidades detectadas.

Puedes ver la última versión del Jenkins complemento en el Jenkins mercado en https://plugins.jenkins.io/amazon-inspector-image-scanner/.

En los siguientes pasos se describe cómo configurar el Jenkins complemento Amazon Inspector.

> **Important**
>
> Antes de completar los siguientes pasos, debe actualizar Jenkins a la versión 2.387.3 o superior para que se ejecute el complemento.

Paso 1. Configura un Cuenta de AWS

Configure una Cuenta de AWS con una función de IAM que permita el acceso a la API de escaneo de Amazon Inspector. Para ver instrucciones, consulte Configuración de una AWS cuenta para usar la integración CI/CD de Amazon Inspector.

Paso 2. Instalación del complemento Amazon Inspector Jenkins

El siguiente procedimiento describe cómo instalar el complemento Amazon Inspector Jenkins desde el Jenkins panel de control.

1. En el panel de control de Jenkins, selecciona Administrar Jenkins y, a continuación, selecciona Administrar complementos.
2. Selecciona Disponible.
3. En la pestaña Disponible, busca Amazon Inspector Scans y, a continuación, instala el complemento.

(Opcional) Paso 3. Agregue credenciales de docker a Jenkins

> **Note**
>
> Agregue credenciales de docker únicamente si la imagen de docker está en un repositorio privado. De lo contrario, omita este paso.

El siguiente procedimiento describe cómo añadir credenciales de docker Jenkins desde el Jenkins panel.

1. En el panel de control de Jenkins, elija Administrar Jenkins, Credenciales y, a continuación, Sistema.
2. Seleccione Credenciales globales y, a continuación, Agregar credenciales.

3. En Tipo, selecciona Nombre de usuario con contraseña.
4. En Ámbito, selecciona Global (Jenkins, nodos, elementos, todos los elementos secundarios, etc.).
5. Introduce tus datos y, a continuación, selecciona Aceptar.

(Opcional) Paso 4. Añadir AWS credenciales

> **Note**
>
> Añada AWS credenciales únicamente si quiere autenticarse en función de un usuario de IAM. De lo contrario, omita este paso.

El siguiente procedimiento describe cómo añadir AWS credenciales desde el Jenkins panel de control.

1. En el panel de control de Jenkins, elija Administrar Jenkins, Credenciales y, a continuación, Sistema.
2. Seleccione Credenciales globales y, a continuación, Agregar credenciales.
3. En Tipo, seleccione AWS Credentials.
4. Introduzca sus datos, incluidos el identificador de la clave de acceso y la clave de acceso secreta, y, a continuación, pulse Aceptar.

Paso 5. Añade compatibilidad con CSS en un Jenkins script

El siguiente procedimiento describe cómo añadir compatibilidad con CSS en un Jenkikns script.

1. Reinicie Jenkins.
2. En el panel, seleccione Administrar Jenkins, Nodes, Built-In Node y, a continuación, Script Console.
3. En el cuadro de texto, añade la línea `ySystem.setProperty("hudson.model.DirectoryBrowserSupport.CSP", "")`, a continuación, selecciona Ejecutar.

Paso 6. Añada Amazon Inspector Scan a su compilación

Puede añadir Amazon Inspector Scan a su compilación añadiendo un paso de compilación en su proyecto o utilizando la canalización declarativa de Jenkins.

Amazon Inspector: escanea tu compilación añadiendo un paso de compilación a tu proyecto

1. En la página de configuración, desplácese hacia abajo hasta Build Steps y elija Add build Steps. A continuación, selecciona Amazon Inspector Scan.
2. Elija entre dos métodos de instalación realizados por el inspector: Automático o Manual.

   a. (Opción 1) Seleccione Automático para descargar la última versión de inspector-sbomgen. Si elige este método, asegúrese de seleccionar la arquitectura de la CPU que coincida con el sistema que ejecuta el complemento.

   b. (Opción 2) Seleccione Manual si desea configurar el binario del generador SBOM de Amazon Inspector para escanearlo. Si elige este método, asegúrese de proporcionar la ruta completa a una versión de inspector-sbomgen descargada anteriormente.

   Para obtener más información, consulte Instalación del Generador de SBOM de Amazon Inspector (Sbomgen) en el Generador de SBOM de Amazon Inspector.
3. Complete lo siguiente para terminar de configurar el paso de compilación de Amazon Inspector Scan:

   a. Introduzca su ID de imagen. La imagen puede ser local, remota o archivada. Los nombres de las imágenes deben seguir la convención de nomenclatura de Docker. Si analiza una imagen exportada, proporcione la ruta al archivo tar esperado. Para ver un ejemplo, consulte las siguientes rutas de identificadores de imágenes:

      i. Para contenedores locales o remotos: `NAME[:TAG|@DIGEST]`

      ii. Para un archivo tar: `/path/to/image.tar`

   b. Seleccione una Región de AWS para enviar la solicitud de análisis.

   c. (Opcional) Para las credenciales de Docker, seleccione su nombre de usuario de Docker. Haga esto solo si la imagen del contenedor está en un repositorio privado.

   d. (Opcional) Puede proporcionar los siguientes métodos de autenticación compatibles: AWS

i. (Opcional) Para el rol de IAM, proporcione un ARN de rol (arn:aws:iam: ::role/). *AccountNumberRoleName*

ii. (Opcional) Para las credenciales de AWS, seleccione ID para autenticarse en función de un usuario de IAM.

iii. (Opcional) Para el nombre del AWS perfil, proporcione el nombre de un perfil para autenticarse con un nombre de perfil.

e. (Opcional) Especifique los umbrales de vulnerabilidad por gravedad. Si se supera el número que especifique durante un análisis, se producirá un error en la compilación de la imagen. Si todos los valores son `0`, la compilación se realizará correctamente, independientemente de si se encuentra alguna vulnerabilidad.

4. Seleccione Guardar.

Añada Amazon Inspector Scan a su compilación mediante la Jenkins canalización declarativa

Puede añadir Amazon Inspector Scan a su compilación mediante la canalización declarativa de Jenkins de forma automática o manual.

Para descargar automáticamente la canalización declarativa de SBOMgen

- Para añadir Amazon Inspector Scan a una compilación, utilice la siguiente sintaxis de ejemplo. Según la arquitectura de sistema operativo que prefiera para descargar el generador SBOM de Amazon Inspector, sustituya *SBOMGEN_SOURCE* por LinuxAMD64 o LinuxARM64. Sustituya *IMAGE_PATH* por la ruta a su imagen (por ejemplo, *alpine:latest*), IAM_ROLE por el *ARN* del rol de IAM que configuró en el paso 1 e *ID por su ID* de credencial si utiliza un repositorio privado. Docker Si lo desea, puede habilitar los umbrales de vulnerabilidad y especificar valores para cada gravedad.

```
pipeline {
   agent any
   stages {
       stage('amazon-inspector-image-scanner') {
           steps {
               script {
               step([
```

```
                $class:
'com.amazon.inspector.jenkins.amazoninspectorbuildstep.AmazonInspectorBuilder',
                sbomgenSource: 'SBOMGEN_SOURCE', // this can be linuxAmd64 or linuxArm64
                archivePath: 'IMAGE_PATH',
                awsRegion: 'REGION',
                iamRole: 'IAM ROLE',
                credentialId: 'Id', // provide empty string if image not in private
repositories
                awsCredentialId: ''AWS ID;',
                awsProfileName: 'Profile Name',
                isThresholdEnabled: false,
                countCritical: 0,
                countHigh: 0,
                countLow: 10,
                countMedium: 5,
               ])
            }
          }
        }
    }
}
```

Para descargar manualmente la canalización declarativa de SBOMgen

- Para añadir Amazon Inspector Scan a una compilación, utilice la siguiente sintaxis de ejemplo. *Sustituya SBOMGEN_PATH por la ruta al generador SBOM de Amazon Inspector que instaló en el paso 3, IMAGE_PATH por la ruta a su imagen (como alpine:latest), IAM_ROLE por el ARN del rol de IAM que configuró en el paso 1 e ID por su ID de credencial si utiliza un repositorio privado.* Docker Si lo desea, puede habilitar los umbrales de vulnerabilidad y especificar valores para cada gravedad.

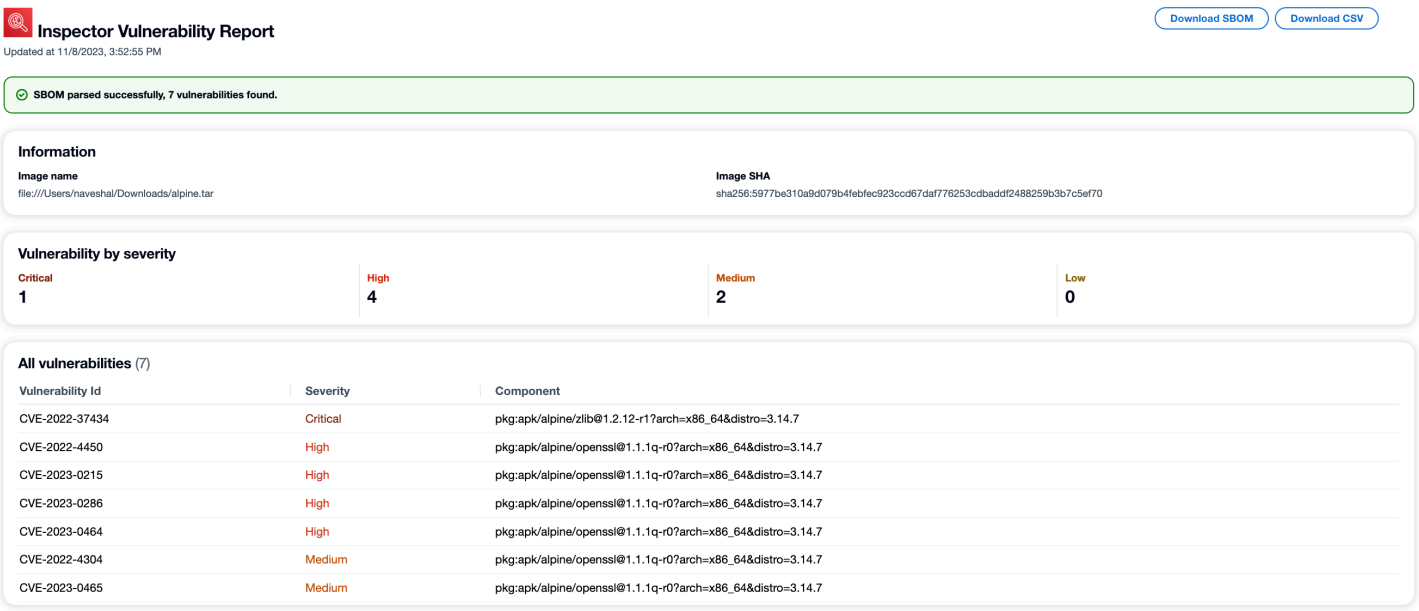
> **Note**
>
> Colóquelo Sbomgen en el directorio de Jenkins y proporcione la ruta al directorio de Jenkins en el complemento (como */opt/folder/arm64/inspector-sbomgen*).

```
pipeline {
    agent any
```

```
    stages {
        stage('amazon-inspector-image-scanner') {
            steps {
                script {
                step([
                $class:
'com.amazon.inspector.jenkins.amazoninspectorbuildstep.AmazonInspectorBuilder',
                sbomgenPath: 'SBOMGEN_PATH',
                archivePath: 'IMAGE_PATH',
                awsRegion: 'REGION',
                iamRole: 'IAM ROLE',
                awsCredentialId: ''AWS ID;',
                credentialId: 'Id;', // provide empty string if image not in private
repositories
                awsProfileName: 'Profile Name',
                isThresholdEnabled: false,
                countCritical: 0,
                countHigh: 0,
                countLow: 10,
                countMedium: 5,
               ])
            }
          }
       }
    }
 }
```

Paso 7. Consulta tu informe de vulnerabilidades de Amazon Inspector

1. Complete una nueva versión de su proyecto.
2. Una vez completada la compilación, selecciona un formato de salida de los resultados. Si selecciona HTML, tiene la opción de descargar una versión JSON, SBOM o CSV del informe. A continuación, se muestra un ejemplo de un informe HTML:



Solución de problemas

Los siguientes son errores habituales que se pueden producir al utilizar el complemento Amazon Inspector ScanJenkins.

No se pudieron cargar las credenciales o se produjo un error de excepción de st

Error:

```
InstanceProfileCredentialsProvider(): Failed to load credentials or sts exception.
```

Resolución

Obtenga `aws_access_key_id` y `aws_secret_access_key` para su cuenta. AWS Configure `aws_access_key_id` y `aws_secret_access_key` en `~/.aws/credentials`.

Error de ruta inspector-sbomgen

Error:

```
Exception:com.amazon.inspector.jenkins.amazoninspectorbuildstep.exception.Sbomge
There was an issue running inspector-sbomgen, is /opt/inspector/inspector-sbomgen the correct path?
```

Solución

Complete el siguiente procedimiento para resolver el problema.

1. Coloque el Inspector-SBOMgen de arquitectura del sistema operativo correcto en el Jenkins directorio Para obtener más información, consulte Amazon Inspector SBOM Generator.
2. Otorgue permisos de ejecución al binario mediante el siguiente comando:. `chmod +x inspector-sbomgen`
3. Proporcione la ruta correcta Jenkins de la máquina en el complemento, como`/opt/folder/arm64/inspector-sbomgen`.
4. Guarde la configuración y ejecute el Jenkins trabajo.

Uso del complemento TeamCity de Amazon Inspector

El complemento TeamCity de Amazon Inspector permite añadir análisis de vulnerabilidades de Amazon Inspector a su canalización de TeamCity. El complemento aprovecha el binario del Generador de SBOM de Amazon Inspector y la API de Amazon Inspector Scan para generar informes detallados al final de la compilación, de modo que pueda investigar y corregir los riesgos antes de la implementación. Los análisis también se pueden configurar para que aprueben o rechacen las ejecuciones en las canalizaciones en función de la cantidad y la gravedad de las vulnerabilidades detectadas.

Amazon Inspector es un servicio de administración de vulnerabilidades ofrecido por AWS que escanea las imágenes de los contenedores en busca de vulnerabilidades de paquetes de sistemas operativos y lenguajes de programación basadas en CVE. Para obtener más información sobre la integración de CI/CD de Amazon Inspector, consulte Integración de análisis de Amazon Inspector en su canalización de CI/CD.

Para obtener una lista de los formatos de imagen de paquetes y contenedores compatibles con el complemento Amazon Inspector, consulte Paquetes y formatos de imagen compatibles.

Puedes ver la última versión del complemento en el TeamCity mercado en https://plugins.jetbrains.com/plugin/23236 - amazon-inspector-scanner. Como alternativa, siga los pasos de cada sección de este documento para configurar el complemento TeamCity de Amazon Inspector:

1. Configura un Cuenta de AWS.

   - Configure una Cuenta de AWS con una función de IAM que permita el acceso a la API de escaneo de Amazon Inspector. Para ver instrucciones, consulte Configuración de una AWS cuenta para usar la integración CI/CD de Amazon Inspector.

2. Instale el omplemento de TeamCity de Amazon Inspector.

   a. Desde su panel de control, vaya a Administración > Complementos.

   b. Busque Amazon Inspector Scans.

   c. Instale el complemento.

3. Instale el Generador de SBOM de Amazon Inspector.

   - Instale el binario del Generador de SBOM de Amazon Inspector en el directorio de su servidor de Teamcity. Para ver instrucciones, consulte Instalación del Generador de SBOM de Amazon Inspector (Sbomgen).

4. Añada un paso de compilación de Amazon Inspector Scan a su proyecto.

   a. En la página de configuración, desplázate hacia abajo hasta Build Steps, selecciona Add build step y, a continuación, selecciona Amazon Inspector Scan.

   b. Configure el paso de compilación de Amazon Inspector Scan rellenando los siguientes detalles:

      - Añada un nombre para el paso.
      - Elija entre dos métodos de instalación del generador Amazon Inspector SBOM: automático o manual.
        - Descarga automáticamente la versión más reciente del generador SBOM de Amazon Inspector en función de la arquitectura del sistema y de la CPU.
        - El manual requiere que proporciones una ruta completa a una versión descargada anteriormente de Amazon Inspector SBOM Generator.

        Para obtener más información, consulte Instalación del generador SBOM de Amazon Inspector (Sbomgen) en Amazon Inspector SBOM Generator.
      - Introduzca su ID de imagen. La imagen puede ser local, remota o archivada. Los nombres de las imágenes deben seguir la convención de nomenclatura de Docker. Si analiza una imagen exportada, proporcione la ruta al archivo tar esperado. Para ver un ejemplo, consulte las siguientes rutas de identificadores de imágenes:
        - Para contenedores locales o remotos: `NAME[:TAG|@DIGEST]`
        - Para un archivo tar: `/path/to/image.tar`
      - Para el rol de IAM, introduzca el ARN del rol que configuró en el paso 1.
      - Seleccione una Región de AWS para enviar la solicitud de análisis.

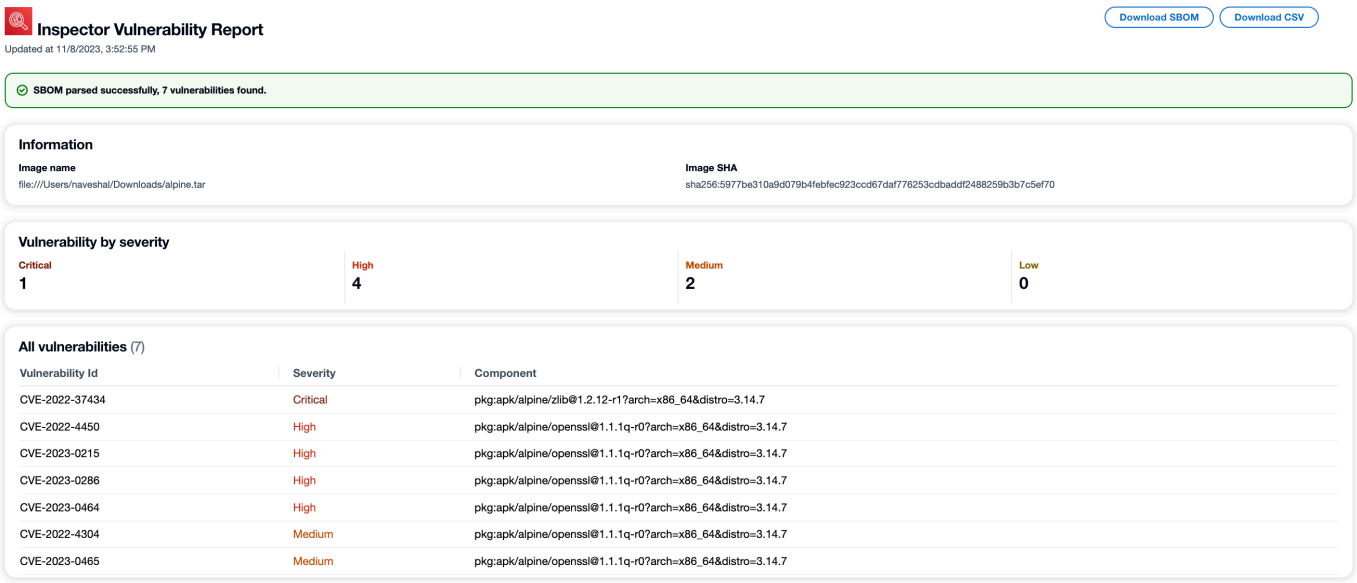
- (Opcional) Para Autenticación de Docker, introduzca su Nombre de usuario y la Contraseña de Docker. Haga esto solo si la imagen del contenedor está en un repositorio privado.
- (Opcional) Para la AWS autenticación, introduzca su ID de clave de acceso y su clave secreta. AWS AWS Haga esto solo si desea autenticarse en función de las AWS credenciales.
- (Opcional) Especifique los umbrales de vulnerabilidad por gravedad. Si se supera el número que especifique durante un análisis, se producirá un error en la compilación de la imagen. Si todos los valores son `0`, la compilación se realizará correctamente, independientemente de la cantidad de vulnerabilidades que se encuentren.

c. Seleccione Guardar.

5. Consulte su informe de vulnerabilidades de Amazon Inspector.

a. Complete una nueva versión de su proyecto.

b. Cuando se complete la compilación, seleccione un formato de salida de los resultados. Al seleccionar HTML, tiene la opción de descargar una versión JSON, SBOM o CSV del informe. El siguiente es un ejemplo de un informe HTML:



Espacios de nombres de CycloneDX de Amazon Inspector

Amazon Inspector ha reservado espacios de nombres y nombres de propiedades de CycloneDX para usarlos con las SBOM producidas por el Generador SBOM de Amazon Inspector y la API de Amazon Inspector Scan. En esta página se documentan todas las propiedades de clave/valor personalizadas que se pueden añadir a los componentes en las SBOM de CycloneDX creadas con las herramientas de Amazon Inspector. Para obtener más información sobre las taxonomías de las propiedades de CycloneDX, consulte la documentación oficial.

Taxonomía de los espacios de nombres de `amazon:inspector:sbom_scanner`

La API de Amazon Inspector Scan utiliza el espacio de nombres de `amazon:inspector:sbom_scanner`. Tiene las siguientes propiedades:

Propiedad	Descripción
`amazon:inspector:sbom_scanner:critical_vulnerabilities`	Recuento del número total de vulnerabilidades de gravedad crítica encontradas en la SBOM.
`amazon:inspector:sbom_scanner:high_vulnerabilities`	Recuento del número total de vulnerabilidades de gravedad alta encontradas en la SBOM.
`amazon:inspector:sbom_scanner:medium_vulnerabilities`	Recuento del número total de vulnerabilidades de gravedad media encontradas en la SBOM.
`amazon:inspector:sbom_scanner:low_vulnerabilities`	Recuento del número total de vulnerabilidades de gravedad baja encontradas en la SBOM.
`amazon:inspector:sbom_scanner:info`	Proporciona el contexto de análisis para un componente determinado, por ejemplo: “Componente analizado: no se ha encontrado ninguna vulnerabilidad”.
`amazon:inspector:sbom_scanner:warning`	Proporciona un contexto que explica por qué no se ha explorado un componente determinado, por ejemplo: “Componente omitido: no se ha proporcionado ninguna dirección URL”.

Propiedad	Descripción
`amazon:inspector:sbom_scanner:fixed_version: component_bom_ref`	Proporciona la versión corregida del componente indicado para la vulnerabilidad en cuestión.
`amazon:inspector:sbom_scanner:exploit_available`	Indica si hay un ataque para la vulnerabilidad en cuestión.
`amazon:inspector:sbom_scanner:exploit_last_seen_in_public`	Indica cuándo se ha visto por última vez en público un ataque relacionado con la vulnerabilidad en cuestión.
`amazon:inspector:sbom_scanner:cisa_kev_date_added`	Indica cuándo se ha agregado la vulnerabilidad al catálogo de vulnerabilidades aprovechadas conocidas de CISA.
`amazon:inspector:sbom_scanner:cisa_kev_date_due`	Indica cuándo vence la corrección de la vulnerabilidad conforme al catálogo de vulnerabilidades aprovechadas conocidas de CISA.
`amazon:inspector:sbom_scanner:path`	La ruta al archivo que ha proporcionado la información del paquete en cuestión.

Taxonomía de los espacios de nombres de **`amazon:inspector:sbom_generator`**

El Generador de SBOM de Amazon Inspector Scan utiliza el espacio de nombres de `amazon:inspector:sbom_generator`. Tiene las siguientes propiedades:

Propiedad	Descripción
`amazon:inspector:sbom_generator:os_hostname`	El nombre de host del sistema que se está inventariando.

Propiedad	Descripción
`amazon:inspector:sbom_generator:kernel_name`	El nombre de kernel del sistema que se está inventariando.
`amazon:inspector:sbom_generator:kernel_version`	La versión de kernel del sistema que se está inventariando.
`amazon:inspector:sbom_generator:cpu_architecture`	La arquitectura de CPU del sistema que se está inventariando, como x86_64.
`amazon:inspector:sbom_generator:image_id`	El hash del archivo de configuración de la imagen del contenedor, también conocido como ID de imagen.
`amazon:inspector:sbom_generator:layer_diff_id`	El hash de la capa de imágenes del contenedor sin comprimir.
`amazon:inspector:sbom_generator:source_file_scanner`	El escáner que encontró el archivo que contiene la información del paquete, por ejemplo: `/var/lib/dpkg/status` .
`amazon:inspector:sbom_generator:source_package_collector`	El recopilador que extrajo el nombre y la versión del paquete de un archivo específico.
`amazon:inspector:sbom_generator:source_path`	La ruta al archivo del que se ha extraído la información del paquete en cuestión.
`amazon:inspector:sbom_generator:is_duplicate_package`	Indica que han encontrado el paquete en cuestión más de un analizador de archivos.
`amazon:inspector:sbom_generator:go_toolchain`	Indica la versión del compilador Go o de la cadena de herramientas utilizada para producir un ejecutable de Go.
`amazon:inspector:sbom_generator:expires_before`	fecha antes de la cual el certificado SSL no es válido.

Propiedad	Descripción
`amazon:inspector:sbom_generator:expires_after`	fecha después de la cual el certificado SSL no es válido.
`amazon:inspector:sbom_generator:is_expired`	un valor booleano que indica si el certificado SSL ha caducado.

Análisis automatizado de recursos con Amazon Inspector

El análisis sin agente de Amazon Inspector para Amazon EC2 se encuentra en una versión preliminar. El uso de la característica de análisis sin agente de Amazon EC2 está sujeto a la sección 2 de las Condiciones del servicio de AWS ("versiones beta y vistas previas").

Amazon Inspector utiliza su propio motor de análisis, diseñado expresamente para ello. El motor supervisa los recursos en busca de vulnerabilidades de software o rutas de red abiertas que puedan afectar a las cargas de trabajo, dar lugar a un uso mal intencionado de los recursos y permitir el acceso no autorizado a los datos. Cuando Amazon Inspector detecta una vulnerabilidad, genera un hallazgo. Los hallazgos incluyen información relacionada con la detección de la vulnerabilidad para ayudarle a corregirla. Puede revisar los hallazgos en la consola de Amazon Inspector y con la API de Amazon Inspector. Para obtener más información, consulte Administración de los hallazgos en Amazon Inspector.

Al activarse, Amazon Inspector detecta automáticamente todos los recursos elegibles y empieza a analizarlos continuamente. Amazon Inspector analiza los recursos en busca de vulnerabilidades de software y exposiciones no deseadas a la red. Amazon Inspector también ejecuta análisis en respuesta a eventos como la instalación de nuevas aplicaciones o parches.

Cuando activa Amazon Inspector por primera vez, la cuenta se inscribe automáticamente en todos los tipos de análisis. En las siguientes secciones se proporcionan detalles específicos acerca de los tipos de análisis de Amazon Inspector. Amazon Inspector clasifica los tipos de análisis según el tipo de recurso afectado por una vulnerabilidad. En las siguientes secciones se indican los recursos que analiza Amazon Inspector, las circunstancias por las que se inician nuevos análisis de recursos y la forma de configurar análisis para cada tipo de recurso.

Temas

Cuando activa Amazon Inspector por primera vez, la cuenta se inscribe automáticamente en los siguientes tipos de análisis: análisis de Amazon EC2, análisis de Amazon ECR y análisis estándar de Lambda. El análisis de código de Lambda es una capa opcional de los análisis de funciones de Lambda y se puede activar en cualquier momento.

Descripción general de los tipos de análisis de Amazon Inspector

Amazon Inspector ofrece una gama de tipos de escaneo diferentes que se centran en tipos de recursos específicos de su AWS entorno.

Análisis de Amazon EC2

Al activar los análisis de Amazon EC2, Amazon Inspector analiza las instancias de Amazon EC2 en busca de vulnerabilidades en los paquetes de sistemas operativos y lenguajes de programación o problemas de accesibilidad de red. Amazon Inspector analiza la instancia de EC2 para detectar vulnerabilidades y riesgos comunes (CVE) y problemas de exposición de la red. Amazon Inspector realiza análisis mediante el uso del agente de SSM instalado en la instancia o mediante instantáneas de las instancias de Amazon EBS. Para obtener más información acerca de los análisis de Amazon EC2, consulte Análisis de instancias de Amazon EC2 con Amazon Inspector.

Análisis de Amazon ECR

Al activar el escaneo Amazon ECR, Amazon Inspector convierte todos los repositorios de contenedores de escaneo básicos de su registro privado en un escaneo mejorado con escaneo continuo. Si lo desea, también puede configurar este parámetro para que analice únicamente de forma automática o para que analice algunos repositorios según reglas de inclusión. Todas las imágenes introducidas en los últimos 30 días o extraídas en los últimos 90 días se escanean inicialmente. Amazon Inspector sigue supervisando las imágenes durante 90 días de forma predeterminada; esta configuración se puede cambiar en cualquier momento. Para obtener más información acerca de los análisis de Amazon ECR, consulte Análisis de imágenes de contenedores de Amazon ECR con Amazon Inspector.

Análisis estándar de Lambda

Al activar el análisis de funciones de Lambda, Amazon Inspector detecta las funciones de Lambda de su cuenta y, de inmediato, comienza a analizarlas en busca de vulnerabilidades. Amazon Inspector analiza las nuevas capas y funciones de Lambda cuando se implementan y vuelve a analizarlas cuando se actualizan o cuando se publican nuevas vulnerabilidades y riesgos

comunes (CVE). Para obtener más información acerca de los análisis de funciones de Lambda, consulte AWS Lambda Funciones de escaneo con Amazon Inspector.

Análisis estándar de Lambda + análisis de código de Lambda

Esta opción combina el análisis estándar de Lambda con el análisis de código de Lambda. Cuando se activa el análisis de código de Lambda, Amazon Inspector detecta las funciones de Lambda y las capas de su cuenta y analiza los recursos en busca de vulnerabilidades de código en las dependencias de paquetes de la aplicación. El análisis de código de Lambda analiza el código personalizado de la aplicación en las funciones de Lambda en busca de vulnerabilidades de código. Estos dos tipos de análisis deben activarse juntos. Para más información, consulte Análisis de código de Lambda con Amazon Inspector.

Activación de un tipo de análisis

Puede activar un nuevo tipo de análisis de Amazon Inspector en cualquier momento. Una vez que actives un tipo de escaneo, Amazon Inspector empezará inmediatamente a escanear los recursos aptos para ese tipo de escaneo. Para obtener una descripción general de los tipos de análisis disponibles, consulte Descripción general de los tipos de análisis de Amazon Inspector. A continuación se explica lo que sucede cuando se activa cada tipo de análisis por primera vez:

- Análisis de Amazon EC2: cuando activa los análisis de Amazon EC2 de Amazon Inspector en una cuenta, Amazon Inspector analiza todas las instancias elegibles de la cuenta en busca de vulnerabilidades de paquetes y problemas de accesibilidad de red. El complemento SSM de Amazon Inspector está instalado en todos los hosts gestionados por SMS. Windows Para obtener más información, consulte Análisis de instancias de Windows. Además, Amazon Inspector crea las siguientes asociaciones de SSM en su cuenta:
  - `InspectorDistributor-do-not-delete`
  - `InspectorInventoryCollection-do-not-delete`
  - `InspectorLinuxDistributor-do-not-delete`
  - `InvokeInspectorLinuxSsmPlugin-do-not-delete`
  - `InvokeInspectorSsmPlugin-do-not-delete`.
- Análisis de Amazon ECR: cuando activa los análisis de imágenes de contenedores de Amazon ECR en una cuenta, el tipo de análisis de Amazon ECR para los repositorios privados de la cuenta cambia de Análisis básico con Amazon ECR a Análisis mejorado con Amazon Inspector. Luego, se escanean todas las imágenes de contenedores de Amazon ECR aptas enviadas en los últimos 30

días o extraídas en los últimos 90 días para detectar vulnerabilidades en los paquetes. Además, la duración del reescaneo de Amazon ECR se establece en 90 días para la fecha de inserción y extracción de imágenes.

- Análisis estándar de Lambda: cuando activa los análisis estándar de Lambda en una cuenta, se analizan todas las funciones de Lambda de la cuenta que se han invocado o actualizado en los últimos 90 días en busca de vulnerabilidades de paquetes. Además, se crea un canal vinculado al CloudTrail servicio en su cuenta.
- Análisis estándar de Lambda + análisis de código de Lambda: estos tipos de análisis de funciones de Lambda se activan conjuntamente. Cuando activa los análisis de código de Lambda en una cuenta, se analizan todas las funciones de Lambda de la cuenta que se han invocado o actualizado en los últimos 90 días en busca de vulnerabilidades de código.

Activación de análisis

Si es el administrador delegado de Amazon Inspector en una AWS organización, puede habilitar automáticamente varios tipos de escaneo de Amazon Inspector para varias cuentas en varias regiones mediante un script shell desarrollado por Amazon Inspector inspector2 - on. enablement-with-cli GitHub Si desea completar este procedimiento para un entorno de varias cuentas a través de la consola, complete los siguientes pasos con la sesión iniciada como administrador delegado de Amazon Inspector.

Console

Activación de análisis

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee activar un nuevo tipo de escaneo.
3. En el panel de navegación, elija Administración de cuentas.
4. En la página Administración de cuentas, seleccione las cuentas en las que desea activar un tipo de análisis.
5. Elija Activar y seleccione el tipo de análisis que desea activar.
6. (Recomendado) Repita estos pasos en cada uno de los tipos Región de AWS de escaneo en los que desee activar ese tipo de escaneo.

API

Ejecute la operación de la API Enable. En la solicitud, proporcione los ID de las cuentas en las que quiera activar los análisis, el token de idempotencia y uno o más valores entre `EC2`, `ECR`, `LAMBDA` y `LAMBDA_CODE` para `resourceTypes`. De esta forma, se activarán los análisis para los tipos de análisis que haya seleccionado.

Análisis de instancias de Amazon EC2 con Amazon Inspector

El análisis sin agente de Amazon Inspector para Amazon EC2 se encuentra en una versión preliminar. El uso de la característica de análisis sin agente de Amazon EC2 está sujeto a la sección 2 de las Condiciones del servicio de AWS (“versiones beta y vistas previas”).

El análisis de Amazon Inspector EC2 extrae metadatos de su instancia de EC2 y, a continuación, los compara con las reglas recopiladas en los avisos de seguridad para generar resultados. Amazon Inspector analiza las instancias en busca de vulnerabilidades en los paquetes y problemas de accesibilidad de la red. Para obtener información acerca de los tipos de hallazgo generados para estos problemas, consulte Tipos de hallazgos en Amazon Inspector.

Amazon Inspector realiza análisis de accesibilidad de la red una vez cada 24 horas, mientras que los análisis de vulnerabilidades de paquetes se realizan con una cadencia variable según el método de análisis asociado a la instancia.

Métodos de análisis

Los análisis de vulnerabilidades de paquetes se pueden realizar mediante un método de análisis basado en agente o sin agente. Estos métodos de análisis determinan cómo y cuándo recopila Amazon Inspector el inventario de software de una instancia de EC2 para analizar las vulnerabilidades de los paquetes. El método basado en agentes se basa en el agente de SSM para recopilar el inventario de software, mientras que el método sin agente utiliza instantáneas de Amazon EBS en lugar de un agente.

Los métodos de análisis utilizados por Amazon Inspector dependen de la configuración del modo de análisis de su cuenta. Para obtener más información, consulte Cómo administrar el modo de análisis.

Para activar los análisis de Amazon EC2, consulte Activación de un tipo de análisis.

Análisis basado en agentes

Los análisis basados en agentes se realizan de forma continua con el agente de SSM en todas las instancias aptas. Para los análisis basados en agentes, Amazon Inspector utiliza asociaciones de SSM y complementos instalados a través de estas asociaciones para recopilar el inventario de software de sus instancias. Además de los análisis de vulnerabilidades de paquetes para paquetes de sistemas operativos, el análisis basado en agentes de Amazon Inspector también puede detectar vulnerabilidades de paquetes de lenguajes de programación de aplicaciones en instancias basadas en Linux mediante Inspección exhaustiva de Amazon Inspector para instancias de Linux de Amazon EC2.

El siguiente proceso explica cómo Amazon Inspector utiliza SSM para recopilar el inventario y realizar análisis basados en agentes:

1. Amazon Inspector crea asociaciones de SSM en su cuenta para recopilar el inventario de sus instancias. Para algunos tipos de instancias (Windows y Linux), estas asociaciones instalan complementos en instancias individuales para recopilar el inventario.
2. Con SSM, Amazon Inspector extrae el inventario de paquetes de una instancia.
3. Amazon Inspector evalúa el inventario extraído y genera resultados con las vulnerabilidades detectadas.

Instancias aptas

Amazon Inspector utilizará el método basado en agentes para analizar una instancia si cumple las condiciones siguientes:

- La instancia tiene un sistema operativo compatible. Para obtener una lista de los sistemas operativos compatibles, consulte la columna Compatibilidad con el análisis basado en agentes de the section called “Sistemas operativos admitidos para el análisis de Amazon EC2”.
- Las etiquetas de exclusión de EC2 de Amazon Inspector no excluyen la instancia de los análisis.
- La instancia está administrada por SSM. Para obtener instrucciones sobre cómo verificar y configurar el agente, consulte Configuración del agente de SSM.

Comportamientos de análisis basados en agentes

Al utilizar el método de análisis basado en agentes, Amazon Inspector inicia nuevos análisis de vulnerabilidades en instancias de EC2 administradas en las siguientes situaciones:

- cuando lanza una nueva instancia de EC2,
- cuando instala nuevo software en una instancia de EC2 existente (Linux y Mac),
- cuando Amazon Inspector añade un nuevo elemento de vulnerabilidades y riesgos comunes (CVE) a su base de datos y ese elemento de CVE es relevante para la instancia de EC2 (Linux y Mac).

Amazon Inspector actualiza el campo Último análisis de una instancia de EC2 cuando se completa el análisis inicial. Después, el campo Último análisis se actualiza cuando Amazon Inspector evalúa el inventario de SSM (de forma predeterminada, cada 30 minutos) o cuando se vuelve a analizar una instancia porque se ha añadido a la base de datos de Amazon Inspector una nueva CVE que afecta a esa instancia.

Puede comprobar la última vez en la que se analizó una instancia de EC2 en busca de vulnerabilidades desde la pestaña Instancias de la página Administración de cuentas o con el comando ListCoverage.

Configuración del agente de SSM

Para que Amazon Inspector detecte las vulnerabilidades de software de una instancia de Amazon EC2 mediante el método de análisis basado en agentes, la instancia debe ser una instancia administrada en Amazon EC2 Systems Manager (SSM). Cuando una instancia está administrada en SSM, esto significa que tiene el agente de SSM instalado y en ejecución y que SSM tiene permiso para administrar la instancia. Si ya utiliza SSM para administrar instancias, no hará falta hacer nada más para los análisis basados en agentes.

De forma predeterminada, el agente de SSM se instala en las instancias de EC2 creadas a partir de algunas imágenes de máquina de Amazon (AMI). Para obtener más información, consulte Acerca del agente de SSM en la Guía del usuario de AWS Systems Manager . Sin embargo, aunque el agente de SSM esté instalado, es posible que deba activarlo manualmente y conceder permisos a SSM para que administre la instancia.

En el procedimiento que se describe a continuación, se indica cómo se puede configurar una instancia de Amazon EC2 como instancia administrada con un perfil de instancia de IAM. También se incluyen enlaces a información más detallada en la Guía del usuario de AWS Systems Manager .

AmazonSSMManagedInstanceCore es la política recomendada cuando se adjunta un perfil de instancia. Esta política incluye todos los permisos necesarios para analizar EC2 con Amazon Inspector.

> **Note**
>
> También puede automatizar la administración de SSM para todas las instancias de EC2 sin tener que utilizar perfiles de instancia de IAM con la configuración de administración de host predeterminada de SSM. Para obtener más información, consulte Configuración de administración de host predeterminada.

Configuración de SSM para una instancia de Amazon EC2

1. Si el proveedor del sistema operativo no ha instalado el agente de SSM, instálelo. Para obtener más información, consulte Uso del agente de SSM.
2. Utilice el AWS CLI para comprobar que el agente SSM se está ejecutando. Para obtener más información, consulte Comprobación del estado del agente de SSM e inicio del agente.
3. Conceda permisos a SSM para que administre la instancia. Para conceder permisos, cree un perfil de instancia de IAM y adjúntelo a la instancia. Se recomienda utilizar la política AmazonSSMManagedInstanceCore, ya que esta política incluye los permisos de distribuidor, inventario y administrador del estado de SSM, los cuales Amazon Inspector necesita para llevar a cabo análisis. Para obtener instrucciones sobre cómo crear un perfil de instancia con estos permisos y adjuntarlo a una instancia, consulte Configuración de permisos de instancia para Systems Manager.
4. (Opcional) Active las actualizaciones automáticas para el agente de SSM. Para obtener más información, consulte Automatización de actualizaciones para el agente de SSM.
5. (Opcional) Configure Systems Manager para que utilice un punto de conexión de Amazon Virtual Private Cloud (Amazon VPC). Para obtener más información, consulte Creación de puntos de conexión de Amazon VPC.

> **Important**
>
> Amazon Inspector requiere una asociación como administrador del estado de Systems Manager en la cuenta para recopilar datos del inventario de aplicaciones de software. Amazon Inspector crea automáticamente una asociación denominada `InspectorInventoryCollection-do-not-delete` si no existe ninguna. Amazon Inspector también requiere una sincronización de los datos de los recursos y crea automáticamente una denominada `InspectorResourceDataSync-do-not-delete` si no existe ninguna. Para obtener más información, consulte Configuración de la sincronización

de datos de recursos para Inventory en la Guía del usuario de AWS Systems Manager . Cada cuenta puede tener un número definido de sincronizaciones de datos de recursos por región. Para obtener más información, consulte Número máximo de sincronizaciones de datos de recursos (Cuenta de AWS por región) en los puntos finales y las cuotas de SSM. Si ha alcanzado el límite, deberá eliminar sincronizaciones de datos de recursos. Para ello, consulte Administración de las sincronizaciones de datos de recursos.

Recursos de SSM creados para los análisis

Amazon Inspector necesita una serie de recursos de SSM en la cuenta para ejecutar análisis de Amazon EC2. La primera vez que active los análisis de Amazon Inspector EC2 se crearán los siguientes recursos:

> **Note**
>
> Si alguno de estos recursos de SSM se elimina mientras el escaneo de Amazon EC2 de Amazon Inspector está activado en su cuenta, Amazon Inspector intentará volver a crearlo en el siguiente intervalo de escaneo.

`InspectorInventoryCollection-do-not-delete`

Se trata de una asociación de Systems Manager State Manager (SSM) que Amazon Inspector utiliza para recopilar el inventario de aplicaciones de software de sus instancias de Amazon EC2. Si la cuenta ya tiene una asociación de SSM para recopilar datos de inventario de `InstanceIds*`, Amazon Inspector la utilizará en vez de crear otra.

`InspectorResourceDataSync-do-not-delete`

Se trata de una sincronización de datos de recursos que Amazon Inspector utiliza para enviar los datos de inventario recopilados de las instancias de Amazon EC2 a un bucket de Amazon S3 propiedad de Amazon Inspector. Para obtener más información, consulte Configuración de la sincronización de datos de recursos para Inventory en la Guía del usuario de AWS Systems Manager .

`InspectorDistributor-do-not-delete`

Se trata de una asociación de SSM que Amazon Inspector utiliza para analizar instancias de Windows. Esta asociación instala el complemento de SSM de Amazon Inspector en las instancias

de Windows. Si el archivo del complemento se elimina sin querer, esta asociación lo reinstala en el próximo intervalo de asociación.

`InvokeInspectorSsmPlugin-do-not-delete`

Se trata de una asociación de SSM que Amazon Inspector utiliza para analizar instancias de Windows. Esta asociación permite a Amazon Inspector iniciar análisis con el complemento. También puede utilizarla para establecer intervalos personalizados de análisis de instancias de Windows. Para obtener más información, consulte Configuración de programaciones para análisis de instancias de Windows.

`InspectorLinuxDistributor-do-not-delete`

Se trata de una asociación SSM que Amazon Inspector utiliza para la inspección profunda de Amazon EC2 Linux. Esta asociación instala el complemento de SSM de Amazon Inspector en las instancias de Linux.

`InvokeInspectorLinuxSsmPlugin-do-not-delete`

Se trata de una asociación de SSM que Amazon Inspector utiliza para la inspección profunda de Amazon EC2 Linux. Esta asociación permite a Amazon Inspector iniciar análisis con el complemento.

> **Note**
>
> Al desactivar el escaneo o la inspección profunda de Amazon EC2 de Amazon Inspector, todos los recursos de SSM se desinstalarán automáticamente de los hosts Linux correspondientes.

Análisis sin agente

Amazon Inspector utiliza un método de análisis sin agente en los casos aptos cuando su cuenta está en el modo de análisis híbrido (que incluye análisis con y sin agente). Para los análisis sin agente, Amazon Inspector utiliza instantáneas de EBS para recopilar un inventario de software de sus instancias. Las instancias analizadas con el método sin agente se analizan para detectar vulnerabilidades tanto de los paquetes del sistema operativo como de los paquetes del lenguaje de programación de aplicaciones.

> **Note**
>
> Al analizar las instancias de Linux en busca de vulnerabilidades en los paquetes de lenguajes de programación de aplicaciones, el método sin agente analiza todas las rutas disponibles, mientras que la exploración basada en agentes solo analiza las rutas predeterminadas y las rutas adicionales que especifique como parte de Inspección exhaustiva de Amazon Inspector para instancias de Linux de Amazon EC2. Esto puede provocar que la misma instancia arroje resultados diferentes en función de si se analiza con el método basado en agentes o sin agente.

El siguiente proceso explica cómo utiliza Amazon Inspector las instantáneas de EBS para recopilar el inventario y realizar análisis sin agente:

1. Amazon Inspector crea una instantánea de EBS de todos los volúmenes asociados a la instancia. Mientras Amazon Inspector la usa, la instantánea se guarda en su cuenta y se etiqueta con `InspectorScan` como clave de etiqueta y con un identificador de análisis único como valor de etiqueta.
2. Amazon Inspector recupera los datos de las instantáneas mediante las API directas de EBS y los evalúa para detectar vulnerabilidades. Se generan resultados con las vulnerabilidades detectadas.
3. Amazon Inspector elimina las instantáneas de EBS que creó en su cuenta.

Instancias aptas

Amazon Inspector utilizará el método basado en agentes para analizar una instancia si cumple las condiciones siguientes:

- La instancia tiene un sistema operativo compatible. Para obtener una lista de los sistemas operativos compatibles, consulte la columna Compatibilidad con el análisis basado en agentes de the section called “Sistemas operativos admitidos para el análisis de Amazon EC2”.
- Las etiquetas de exclusión de EC2 de Amazon Inspector no excluyen la instancia de los análisis.
- El estado de la instancia es, o. `Unmanaged EC2 instance` `Stale inventory` `No inventory`
- La instancia está respaldada por EBS y tiene uno de los siguientes formatos de sistema de archivos:
  - `ext3`
  - `ext4`

- `xfs`

Comportamientos de análisis sin agente

Cuando su cuenta está configurada para el análisis híbrido, Amazon Inspector realiza análisis sin agente de las instancias aptas cada 24 horas. Amazon Inspector detecta y analiza las nuevas instancias aptas cada hora, lo que incluye instancias nuevas sin agentes de SSM o instancias preexistentes con estados que han cambiado a `SSM_UNMANAGED`.

Amazon Inspector actualiza el campo Último análisis de una instancia de Amazon EC2 cada vez que analiza las instantáneas extraídas de una instancia tras un análisis sin agente.

Puede comprobar la última vez en la que se analizó una instancia de EC2 en busca de vulnerabilidades desde la pestaña Instancias de la página Administración de cuentas o con el comando ListCoverage.

Cómo administrar el modo de análisis

El modo de análisis de EC2 determina qué métodos de análisis utilizará Amazon Inspector al realizar análisis de EC2 en su cuenta. Puede ver el modo de análisis de su cuenta en la página de configuración de análisis de EC2, en Configuración general. Las cuentas independientes o los administradores delegados de Amazon Inspector pueden cambiar el modo de análisis. Cuando se configura el modo de análisis como administrador delegado de Amazon Inspector, dicho modo se configura para las cuentas de todos los miembros de su organización. Amazon Inspector tiene los siguientes modos de análisis:

Análisis basado en agentes: en este modo, Amazon Inspector utilizará exclusivamente el método de análisis basado en agentes para buscar vulnerabilidades en los paquetes. Este modo solo analiza las instancias administradas por SSM en su cuenta, pero tiene la ventaja de ofrecer análisis continuos en respuesta a nuevas CVE o a cambios en las instancias. El análisis basado en agentes también ofrece inspección profunda de Amazon Inspector para las instancias aptas. Este es el modo de análisis predeterminado para las cuentas recién activadas.

Análisis híbrido: en este modo de análisis, Amazon Inspector utiliza una combinación de los dos métodos, el basado en agentes y el método sin agente, para buscar vulnerabilidades en los paquetes. Para las instancias de EC2 aptas que tienen el agente SSM instalado y configurado, Amazon Inspector utiliza el método basado en agentes. En el caso de las instancias aptas que no estén gestionadas por SSM, Amazon Inspector utilizará el método sin agente para las instancias compatibles respaldadas por EBS.

Cambio del modo de análisis

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee cambiar el modo de escaneo de EC2.
3. En el panel de navegación lateral, en Configuración general, seleccione Configuración de análisis de EC2.
4. En Modo de análisis, seleccione Editar.
5. Elija un modo de análisis y, a continuación, seleccione Guardar cambios.

Exclusión de instancias de los análisis de Amazon Inspector

Puede etiquetar determinadas instancias para excluirlas de los análisis de Amazon Inspector. Excluir instancias de los análisis ayuda a evitar recibir alertas no procesables. No se le cobrará por las instancias excluidas.

Para excluir una instancia de EC2 de los análisis, etiquete esa instancia con la siguiente clave:

- `InspectorEc2Exclusion`

El valor es opcional.

Para obtener más información sobre cómo agregar etiquetas, consulte Etiquetar los recursos de Amazon EC2.

Además, puede excluir un volumen de EBS cifrado de los escaneos sin agente etiquetando con la etiqueta la AWS KMS clave utilizada para cifrar ese volumen. `InspectorEc2Exclusion` Para obtener más información acerca del etiquetado, consulte Claves de etiquetado

Sistemas operativos compatibles

Amazon Inspector analiza las instancias de EC2 compatibles con Mac, Windows y Linux en busca de vulnerabilidades en los paquetes del sistema operativo. En el caso de las instancias de Linux, Amazon Inspector puede generar hallazgos sobre paquetes de lenguajes de programación de la aplicación mediante la Inspección exhaustiva de Amazon Inspector para instancias de Linux de Amazon EC2. En el caso de las instancias de Mac y Windows, solo se analizan los paquetes de sistemas operativos.

Para obtener información sobre los sistemas operativos compatibles, incluido el sistema operativo que se puede analizar sin un agente SSM, consulte Sistemas operativos admitidos para el análisis de Amazon EC2.

Inspección exhaustiva de Amazon Inspector para instancias de Linux de Amazon EC2

Amazon Inspector amplía su cobertura de digitalización de Amazon EC2 para incluir la inspección profunda. Mediante una inspección exhaustiva, Amazon Inspector detecta las vulnerabilidades de los paquetes de lenguajes de programación de aplicaciones en sus instancias Amazon EC2 basadas en Linux.

Amazon Inspector analiza las rutas predeterminadas de las bibliotecas de paquetes de lenguajes de programación. También puede configurar rutas personalizadas además de las rutas predeterminadas. Para obtener más información, consulte Rutas personalizadas para la inspección profunda de Amazon Inspector.

Amazon Inspector realiza escaneos de inspección exhaustivos con los datos recopilados con el complemento Amazon Inspector SSM. Para administrar el complemento y realizar una inspección exhaustiva de Linux, Amazon Inspector crea automáticamente la siguiente asociación de SSM `InvokeInspectorLinuxSsmPlugin-do-not-delete` en su cuenta. Esto ocurre cuando Amazon Inspector activa la inspección profunda.

Amazon Inspector recopila datos actualizados del inventario de aplicaciones procedentes de instancias configuradas para la inspección profunda cada 6 horas.

Para ver una lista de los lenguajes de programación que admite Amazon Inspector para la inspección profunda, consulte Lenguajes de programación compatibles: Amazon EC2 Deep Inspection.

> **Note**
>
> La inspección profunda no es compatible con instancias de Windows o Mac.

Activación y desactivación de la inspección profunda

> **Note**
>
> La inspección profunda se activa automáticamente como parte del análisis de Amazon EC2 en las cuentas en las que se activa Amazon Inspector a partir del 17 de abril de 2023.

Puede comprobar si la inspección profunda está activa en una cuenta Amazon en la consola de Amazon Inspector. Para ello, vaya a columna Análisis de EC2 de la página Administración de cuentas. Si la inspección profunda no está activa, se mostrará el mensaje Activada (inspección profunda desactivada). Para comprobar el estado de activación programáticamente, utilice la API GetEc2DeepInspectionConfiguration. O bien, para varias cuentas, use la API BatchGetMemberEc2DeepInspectionStatus.

Si activó Amazon Inspector antes del 17 de abril de 2023, puede desactivar la inspección profunda a través del banner de la consola o con la API UpdateEc2DeepInspectionConfiguration. Si es administrador delegado de una organización en Amazon Inspector, puede utilizar la API BatchUpdateMemberEc2DeepInspectionStatus para activar la inspección profunda en su cuenta y en otras cuentas de miembros.

Puede desactivar la inspección profunda a través de la API UpdateEc2DeepInspectionConfiguration. Las cuentas de miembros de una organización no pueden desactivar la inspección profunda. Debe hacerlo el administrador delegado para las cuentas de miembros con la API BatchUpdateMemberEc2DeepInspectionStatus.

Acerca del complemento de SSM de Amazon Inspector para Linux

Amazon Inspector utiliza el complemento de SSM de Amazon Inspector para realizar inspecciones profundas de las instancias de Linux. El complemento de SSM de Amazon Inspector se instala automáticamente en el siguiente directorio de las instancias de Linux: `/opt/aws/inspector/bin`. El nombre del archivo ejecutable es `inspectorssmplugin`.

> **Note**
>
> Amazon Inspector utiliza Systems Manager Distributor para implementar el complemento en la instancia de Amazon EC2. Systems Manager Distributor admite los sistemas operativos que se indican en la sección Plataformas de paquetes y arquitecturas admitidas de la guía de Systems Manager. El sistema operativo de la instancia de Amazon EC2 debe ser compatible

con Systems Manager Distributor y Amazon Inspector para que este pueda realizar análisis de inspección profunda.

Amazon Inspector crea los siguientes directorios de archivos para administrar los datos recopilados de la inspección profunda con el complemento de SSM de Amazon Inspector:

- `/opt/aws/inspector/var/input`
- `/opt/aws/inspector/var/output`
  - El archivo `packages.txt` de este directorio almacena las rutas completas a los paquetes detectados durante la inspección profunda. Si Amazon Inspector detecta el mismo paquete varias veces en la instancia, en este archivo se indica la ubicación en la que se encontró cada paquete.

Amazon Inspector almacena los registros para el complemento en el directorio `/var/log/amazon/inspector`.

Desinstalación del complemento de SSM de Amazon Inspector

Si el archivo `inspectorssmplugin` se elimina sin querer, esta asociación de SSM `InspectorLinuxDistributor-do-not-delete` intenta reinstalar el complemento en el próximo intervalo de asociación.

Si desactiva el escaneo de Amazon EC2, el complemento se desinstalará automáticamente de todos los hosts Linux.

Rutas personalizadas para la inspección profunda de Amazon Inspector

Puede configurar rutas personalizadas para que Amazon Inspector las busque cuando realice una inspección exhaustiva de sus instancias Amazon EC2 de Linux. Al añadir una ruta personalizada, Amazon Inspector analiza los paquetes de ese directorio y de todos sus subdirectorios.

Todas las cuentas pueden definir hasta 5 rutas personalizadas en su cuenta. Si es administrador delegado de una organización, puede definir 5 rutas adicionales que se aplicarán a toda la organización. En total, se analizan hasta 10 rutas personalizadas por cuenta en la organización.

Amazon Inspector analiza todas las rutas personalizadas, así como las siguientes rutas predeterminadas que se analizan para todas las cuentas:

- `/usr/lib`

- `/usr/lib64`
- `/usr/local/lib`
- `/usr/local/lib64`

> **Note**
>
> Las rutas personalizadas deben ser rutas locales. Amazon Inspector no analiza rutas de red asignadas como los montajes de Network File System (NFS) o los montajes de sistemas de archivo de Amazon S3.

Formato de rutas personalizadas

A continuación se muestra un ejemplo del formato de una ruta personalizada: `/home/usr1/project01`

Las rutas personalizadas no pueden tener más de 256 caracteres.

Existe un límite de 5000 paquetes por instancia y un límite máximo de tiempo de recopilación de datos de inventarios de paquetes de 15 minutos. Le recomendamos que elija rutas personalizadas para superar estos límites.

Configuración de una ruta personalizada en la consola

Console

Inicie sesión como administrador delegado de Amazon Inspector y siga los pasos siguientes para agregar rutas personalizadas a su organización.

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee activar el escaneado estándar Lambda.
3. En el panel de navegación lateral, en Configuración general, seleccione Configuración de análisis de EC2.
4. En Rutas personalizadas para su propia cuenta, seleccione Editar para agregar rutas a su cuenta. Si es administrador delegado, puede elegir Editar en el panel Rutas personalizadas para su organización para agregar rutas personalizadas a todas las cuentas de la organización.

5. Introduzca las rutas personalizadas en los cuadros de texto.
6. Elija Guardar para guardar las rutas personalizadas. Amazon Inspector incluirá estas rutas en su próxima inspección profunda.

API

Ejecute el comando UpdateEc2DeepInspectionConfiguration. Para `packagePaths`, especifique una matriz de rutas para el análisis.

Lenguajes de programación admitidos

En el caso de las instancias de Linux, la inspección profunda de Amazon Inspector puede arrojar resultados sobre los paquetes de lenguajes de programación de aplicaciones, además de las vulnerabilidades en los paquetes del sistema operativo. En el caso de las instancias de Mac y Windows, solo se analizan los paquetes de sistemas operativos.

Para obtener más información y ver una lista de los lenguajes de programación compatibles, consulte Lenguajes de programación compatibles con la inspección profunda de Amazon Inspector.

Análisis de instancias de EC2 de Windows con Amazon Inspector

> **Note**
>
> El 31 de agosto de 2022, Amazon Inspector amplió la cobertura de análisis de Amazon EC2 para incluir instancias de EC2 que ejecutan Windows.

Amazon Inspector detecta automáticamente todas las instancias de Windows compatibles y las incluye en análisis continuos sin que tenga que hacer nada más. Para conocer las instancias compatibles, consulte Sistemas operativos admitidos para el análisis de Amazon EC2.

A diferencia de los análisis de instancias basadas en Linux, Amazon Inspector ejecuta análisis de Windows en intervalos regulares. Las instancias de Windows se analizan inicialmente en cuanto se detectan y, luego, cada 6 horas. No obstante, el intervalo de análisis predeterminado de 6 horas puede modificarse. Para obtener más información, consulte Configuración de programaciones para análisis de instancias de Windows. A continuación se incluye una descripción general acerca de los análisis de instancias de Windows con Amazon Inspector:

1. Cuando se activa el análisis de Amazon EC2, Amazon Inspector crea nuevas asociaciones de SSM para los recursos de Windows: `InspectorDistributor-do-not-delete`, `InspectorInventoryCollection-do-not-delete` y `InvokeInspectorSsmPlugin-do-not-delete`.
2. La asociación `InspectorDistributor-do-not-delete` SSM usa el documento `AWS-ConfigureAWSPackage` SSM y el paquete `AmazonInspector2-InspectorSsmPlugin` SSM Distributor para instalar el complemento SSM Amazon Inspector en sus instancias. Windows Para obtener más información, consulte Acerca del complemento SSM de Amazon Inspector para Windows.
3. La asociación `InvokeInspectorSsmPlugin-do-not-delete` SSM ejecuta el complemento Amazon Inspector SSM a intervalos regulares para recopilar datos de instancias y generar las conclusiones de Amazon Inspector. De forma predeterminada, este intervalo es de 6 horas. No obstante, puede configurar una expresión cron o una expresión de frecuencia en la asociación con SSM para personalizar este intervalo. Para obtener más información, consulte Referencia: expresiones cron y rate para Systems Manager en la Guía del usuario de AWS Systems Manager .

> **Note**
>
> Amazon Inspector clasifica los archivos de definición de Open Vulnerability and Assessment Language (OVAL) en el bucket de S3 `inspector2-oval-prod-REGION`. Este bucket de S3 contiene las definiciones de OVAL que se utilizan en los análisis y no pueden modificarse. Si se modifica este valor, Amazon Inspector no podrá analizar las nuevas CVE cuando se publiquen.

Requisitos de los análisis de Amazon Inspector para instancias de Windows

Para analizar una instancia de Windows, Amazon Inspector requiere que la instancia cumpla con los siguientes criterios:

- La instancia debe ser una instancia administrada en SSM. Para obtener las instrucciones de configuración de instancias para análisis, consulte Configuración del agente de SSM.
- El sistema operativo de la instancia debe ser un sistema operativo compatible con Windows. Para ver una lista completa de los sistemas operativos admitidos, consulte Sistemas operativos admitidos para el análisis de Amazon EC2.

- La instancia tiene instalado el complemento Amazon Inspector SSM. Amazon Inspector instala automáticamente el complemento Amazon Inspector SSM para las instancias gestionadas al detectarlas. Consulte la siguiente sección para obtener información acerca del complemento.

> **Note**
>
> Si el host se ejecuta en una Amazon VPC sin conexión externa a Internet, el análisis de Windows obliga a que el host pueda acceder a los puntos de conexión regionales de Amazon S3. Para aprender a configurar un punto de conexión de Amazon VPC en Amazon S3, consulte Creación de un punto de conexión de la puerta de enlace en la Guía del usuario de Amazon Virtual Private Cloud. Si su política de puntos de conexión de Amazon VPC restringe el acceso a buckets S3 externos, debe permitir específicamente el acceso al bucket que Amazon Inspector mantiene en su lugar y Región de AWS que almacena las definiciones de OVAL utilizadas para evaluar su instancia. Este bucket tiene el siguiente formato: `inspector2-oval-prod-`*`REGION`*.

Acerca del complemento SSM de Amazon Inspector para Windows

El complemento Amazon Inspector SSM es necesario para que Amazon Inspector escanee sus Windows instancias. El complemento SSM de Amazon Inspector se instala automáticamente en Windows `C:\Program Files\Amazon\Inspector` las instancias y el archivo binario ejecutable recibe un nombre`InspectorSsmPlugin.exe`.

Las siguientes ubicaciones de archivos se crean para almacenar los datos que recopila el complemento SSM de Amazon Inspector:

- `C:\ProgramData\Amazon\Inspector\Input`
- `C:\ProgramData\Amazon\Inspector\Output`
- `C:\ProgramData\Amazon\Inspector\Logs`

> **Note**
>
> De forma predeterminada, el complemento SSM de Amazon Inspector se ejecuta con una prioridad inferior a la normal.

Desinstalación del complemento de SSM de Amazon Inspector

Si el archivo `InspectorSsmPlugin.exe` se elimina sin querer, esta asociación de SSM de `InspectorDistributor-do-not-delete` reinstala el complemento en el próximo intervalo de análisis de Windows. Si desea desinstalar el complemento SSM de Amazon Inspector, puede utilizar la acción Desinstalar del `AmazonInspector2-ConfigureInspectorSsmPlugin` documento.

Además, el complemento SSM de Amazon Inspector se desinstalará automáticamente de todos los Windows hosts si desactiva el escaneo de Amazon EC2.

> **Note**
>
> Si desinstala el agente SSM antes de desactivar Amazon Inspector, el complemento SSM de Amazon Inspector permanecerá en el Windows host pero ya no enviará datos al complemento SSM de Amazon Inspector. Para obtener más información, consulte Desactivación de Amazon Inspector.

Configuración de programaciones para análisis de instancias de Windows

Si desea personalizar el tiempo transcurrido entre análisis de instancias de Amazon EC2 de Windows, configure una expresión cron o una expresión de frecuencia para la asociación `InvokeInspectorSsmPlugin-do-not-delete` con SSM. Para obtener más información, consulte Referencia: expresiones cron y rate para Systems Manager en la Guía del usuario de AWS Systems Manager o utilice las siguientes instrucciones.

Seleccione uno de los siguientes ejemplos de código para modificar la cadencia de análisis de las instancias de Windows desde el valor predeterminado de 6 horas hasta 12 horas con una expresión de frecuencia o una expresión cron.

Los siguientes ejemplos requieren que utilice el AssociationIdpara la asociación nombrada. `InvokeInspectorSsmPlugin-do-not-delete` Puede recuperar el suyo AssociationIdejecutando el siguiente AWS CLI comando:

```
$ aws ssm list-associations --association-filter-list
 "key=AssociationName,value=InvokeInspectorSsmPlugin-do-not-delete" --region us-east-1
```

> **Note**
>
> El AssociationIdes regional, por lo que primero debes recuperar un identificador único para cada uno Región de AWS. A continuación, ejecute el comando para modificar la cadencia de análisis en cada región donde quiera configurar una programación de análisis personalizada para las instancias de Windows.

Example rate expression

```
$ aws ssm update-association \
--association-id "YourAssociationId" \
--association-name "InvokeInspectorSsmPlugin-do-not-delete" \
--schedule-expression "rate(12 hours)"
```

Example cron expression

```
$ aws ssm update-association \
--association-id "YourAssociationId" \
--association-name "InvokeInspectorSsmPlugin-do-not-delete" \
--schedule-expression "cron(0 0/12 * * ? *)"
```

Análisis de imágenes de contenedores de Amazon ECR con Amazon Inspector

Amazon Inspector analiza las imágenes de contenedores almacenadas en Amazon ECR en busca de vulnerabilidades de software para generar hallazgos de vulnerabilidades de paquetes. Para obtener información acerca de los tipos de hallazgo generados para estos problemas, consulte Tipos de hallazgos en Amazon Inspector.

Al activar los análisis de Amazon Inspector para Amazon ECR, se configura Amazon Inspector como servicio de análisis preferido para su registro privado. Amazon Inspector reemplaza los análisis básicos predeterminados, que se ofrecen de forma gratuita en Amazon ECR, por análisis mejorados, que se ofrecen y facturan a través de Amazon Inspector.

Los análisis mejorados de Amazon Inspector le ofrecen la ventaja de analizar vulnerabilidades tanto de sistemas operativos como de paquetes de lenguajes de programación en el nivel de registro.

Puede revisar los hallazgos descubiertos a partir de análisis mejorados en el nivel de imagen, para cada capa de la imagen, en la consola de Amazon ECR. Además, puedes revisar estos resultados y trabajar con ellos en otros servicios que no están disponibles para los resultados de digitalización básicos, como AWS Security Hub Amazon EventBridge. Puede ver los hallazgos detectados mediante escaneos en la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home. Para obtener información sobre cómo trabajar con hallazgos, consulte Administración de los hallazgos en Amazon Inspector.

Para ver las instrucciones de activación de análisis de Amazon ECR, consulte Activación de un tipo de análisis.

Comportamientos de los análisis de Amazon ECR

Cuando activas el escaneo ECR por primera vez y tu repositorio está configurado para el escaneo continuo, Amazon Inspector detecta todas las imágenes aptas que hayas enviado en un plazo de 30 días o que hayas extraído en los últimos 90 días. A continuación, Amazon Inspector escanea las imágenes detectadas y establece su estado de escaneo en `active`. Amazon Inspector sigue supervisando las imágenes siempre que se hayan insertado o extraído en los últimos 90 días (de forma predeterminada) o dentro del tiempo de reescaneo de ECR que configure. Para obtener más información, consulte Configuración de la duración de la redigitalización del ECR.

Para un escaneo continuo, Amazon Inspector inicia nuevos escaneos de vulnerabilidades de las imágenes de los contenedores en las siguientes situaciones:

- cada vez que se inserta una nueva imagen de contenedor,
- cada vez que Amazon Inspector agrega un nuevo elemento de vulnerabilidades y riesgos comunes (CVE) a su base de datos y una CVE es relevante para la imagen de contenedor (solo para análisis continuos).

Si configura su repositorio para escanearlas automáticamente, las imágenes solo se escanearán cuando las inserte.

Puede comprobar la última vez en la que se revisó una imagen de contenedor en busca de vulnerabilidades desde la pestaña Imágenes de contenedores de la página Administración de cuentas o con la API ListCoverage. Amazon Inspector actualiza el campo Fecha del último análisis de una imagen de Amazon ECR en respuesta a los siguientes eventos:

- cuando Amazon Inspector completa un análisis inicial de una imagen de contenedor,

- cuando Amazon Inspector vuelve a analizar una imagen de contenedor porque se ha agregado a la base de datos de Amazon Inspector un nuevo elemento de vulnerabilidades y riesgos comunes (CVE) que afecta a dicha imagen de contenedor.

Sistemas operativos y tipos de medios compatibles

Para obtener información acerca de los sistemas operativos compatibles, consulte Sistemas operativos admitidos para el análisis de Amazon ECR.

Los análisis de Amazon Inspector de repositorios de Amazon ECR cubren los siguientes tipos de medios compatibles:

- `"application/vnd.docker.distribution.manifest.v1+json"`
- `"application/vnd.docker.distribution.manifest.v1+prettyjws"`
- `"application/vnd.oci.image.manifest.v1+json"`
- `"application/vnd.docker.distribution.manifest.v2+json"`

> **Note**
>
> No se admiten imágenes de reserva ni imágenes `DockerV2ListMediaType`.

Configuración de los análisis mejorados para repositorios de Amazon ECR

Al activar los análisis de Amazon Inspector para las imágenes de contenedores de Amazon ECR, se modifica el valor de configuración de análisis de su registro privado. El tipo de análisis del registro cambia de Análisis básico a Análisis mejorado, proporcionado por Amazon Inspector. Para obtener más información, consulte Escaneo de imágenes en la Guía del usuario de Amazon ECR.

Puede administrar la configuración de los análisis mejorados en el nivel de repositorio de ECR. Puede elegir análisis continuos o análisis automáticos para sus repositorios. Los análisis continuos incluyen análisis automáticos y análisis repetidos y automatizados. Los análisis automáticos solo se producen la primera vez que inserta una imagen. Para ambas opciones, puede limitar el alcance de los análisis mediante filtros de inclusión. De forma predeterminada, la configuración se establece en Analizar todos los repositorios de forma continua la primera vez que activa el análisis mejorado.

Configuración del análisis mejorado

1. Abra la consola de Amazon ECR en https://console.aws.amazon.com/ecr/.
2. En el Región de AWS selector de la esquina superior derecha de la página, selecciona la región en la que se encuentran los repositorios que vas a digitalizar.
3. En el panel de navegación, elija Registro privado y, a continuación, Analizando.
4. En Tipo de análisis, asegúrese de que se haya seleccionado Análisis mejorado. Si no lo está, seleccione Análisis mejorado.

   De forma predeterminada, se selecciona la opción Analizar todos los repositorios de forma continua, lo que activa la cobertura completa de análisis de Amazon Inspector para todos los repositorios.
5. Desmarque la opción Analizar todos los repositorios de forma continua para filtrar los repositorios que se analizan de forma continua o automática.

Para obtener más información sobre cómo configurar el análisis mejorado, consulte Uso de escaneos mejorados en la guía del usuario de Amazon ECR.

Configuración de la duración de la redigitalización del ECR

La configuración de duración de la redigitalización del ECR determina durante cuánto tiempo Amazon Inspector monitorea continuamente las imágenes de los contenedores en los repositorios. Puede configurar la duración del nuevo escaneo para la fecha de inserción y la fecha de extracción de la imagen. La duración predeterminada del escaneo para las cuentas nuevas, incluidas las nuevas cuentas agregadas a una organización, es de 90 días.

Fecha y duración de la inserción de la imagen

La duración de la fecha de inserción de la imagen determina cuánto tiempo Amazon Inspector monitorea continuamente las imágenes después de haberlas enviado a los repositorios tras la última fecha de extracción. Las siguientes opciones están disponibles como duraciones para volver a digitalizar:

- 14 días
- 30 días
- 60 días
- 90 días (predeterminado)

- 180 días
- Vida útil

Fecha y duración de la extracción de la imagen

La duración de la fecha de extracción de imágenes determina cuánto tiempo Amazon Inspector monitorea continuamente las imágenes después de la última fecha de extracción. Las siguientes opciones están disponibles como duraciones para volver a escanear:

- 14 días
- 30 días
- 60 días
- 90 días (predeterminado)
- 180 días

Amazon Inspector seguirá supervisando y volviendo a escanear una imagen siempre que se haya insertado o arrastrado dentro de las fechas de inserción y extracción configuradas. Si la imagen no se ha insertado o extraído dentro de las fechas de inserción y extracción configuradas, Amazon Inspector deja de monitorizarla.

> **Note**
>
> Cuando Amazon Inspector deja de monitorizar una imagen, establece el código de estado del escaneo de la imagen en `inactive` y el código de motivo en `expired`. A continuación, programa el cierre de todas las imágenes encontradas asociadas.

Establezca la duración del nuevo escaneo para que se adapte mejor a su entorno. Por ejemplo, si crea imágenes con frecuencia, elija una duración de escaneo más corta. Del mismo modo, si usa imágenes durante períodos de tiempo prolongados, elija una duración de escaneo más larga.

Al configurar la duración del nuevo escaneo desde una cuenta de administrador delegado, Amazon Inspector aplica la configuración a todas las cuentas de los miembros de la organización.

Para configurar la duración de la redigitalización del ECR

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.

2. En el panel de navegación, seleccione Configuración general y, a continuación, seleccione Configuración de digitalización ECR.
3. En la configuración de digitalización con ECR, en Duración de la nueva digitalización con ECR, elija la duración de la fecha de inserción de la imagen y la duración de la fecha de extracción de la imagen que desee establecer.
4. Seleccione Guardar. La nueva configuración se aplicará inmediatamente.

> **Note**
>
> Si aumentas la duración de la fecha de inserción, Amazon Inspector aplica el cambio a todas las imágenes escaneadas activamente en los repositorios configurados para el escaneo continuo. Sin embargo, las imágenes inactivas permanecen inactivas, incluso si las ha colocado dentro de la nueva duración.

AWS Lambda Funciones de escaneo con Amazon Inspector

El soporte de Amazon Inspector para AWS Lambda las funciones proporciona evaluaciones continuas y automatizadas de las vulnerabilidades de seguridad para las funciones y capas de Lambda. Amazon Inspector ofrece dos tipos de análisis para Lambda. Estos tipos de análisis examinan distintos tipos de vulnerabilidades.

Análisis estándar de Lambda con Amazon Inspector

Se trata del tipo de análisis de Lambda predeterminado. El análisis estándar de Lambda examina las dependencias de aplicaciones en una función de Lambda y sus capas en busca de vulnerabilidades de paquetes. Para obtener más información, consulte Análisis estándar de Lambda.

Análisis de código de Lambda con Amazon Inspector

Este tipo de análisis examina el código personalizado de la aplicación en las capas y funciones en busca de vulnerabilidades de código. Puede activar solo el análisis estándar de Lambda o activar este junto al análisis de código de Lambda. Para obtener más información, consulte Análisis de código de Lambda con Amazon Inspector.

Al activar el escaneo Lambda, Amazon Inspector crea los siguientes canales AWS CloudTrail vinculados a servicios en su cuenta:

- `cloudtrail:CreateServiceLinkedChannel`
- `cloudtrail:DeleteServiceLinkedChannel`

Amazon Inspector gestiona estos canales y los utiliza para supervisar tus CloudTrail eventos y escanearlos. Para obtener más información sobre los canales vinculados a servicios, consulte Visualización de canales vinculados a servicios CloudTrail mediante la CLI. AWS

> **Note**
>
> Los canales vinculados a servicios creados por Amazon Inspector te permiten ver CloudTrail los eventos de tu cuenta como si tuvieras una CloudTrail ruta; sin embargo, te recomendamos que crees la tuya propia CloudTrail para gestionar los eventos de tu cuenta.

Para ver las instrucciones de activación de análisis de Lambda, consulte Activación de un tipo de análisis.

Comportamientos de los análisis de funciones de Lambda

Tras activarse, Amazon Inspector analiza todas las funciones de Lambda invocadas o actualizadas en los últimos 90 días en la cuenta. Amazon Inspector inicia análisis de funciones de Lambda en busca de vulnerabilidades en las siguientes situaciones:

- en cuanto Amazon Inspector detecta una función de Lambda,
- cuando implementa una nueva función de Lambda en el servicio de Lambda,
- cuando implementa una actualización en el código de la aplicación o las dependencias de una función de Lambda o sus capas,
- siempre que Amazon Inspector añade un nuevo elemento de vulnerabilidades y riesgos comunes (CVE) a su base de datos y ese elemento de CVE es relevante para la función.

Amazon Inspector supervisa todas las funciones de Lambda a lo largo de su vida útil hasta que se eliminan o se excluyen de los análisis.

Puede comprobar la última vez en la que se revisó una función de Lambda en busca de vulnerabilidades desde la pestaña Funciones de Lambda de la página Administración de cuentas o con la API ListCoverage. Amazon Inspector actualiza el campo Fecha del último análisis de una función de Lambda en respuesta a los siguientes eventos:

- cuando Amazon Inspector completa un análisis inicial de una función de Lambda,
- cuando se actualiza una función de Lambda,
- cuando Amazon Inspector vuelve a analizar una función de Lambda porque se ha añadido a la base de datos de Amazon Inspector un nuevo elemento de CVE que afecta a la función.

Tiempos de ejecución admitidos y funciones elegibles

Amazon Inspector admite distintos tiempos de ejecución para el análisis estándar y el análisis de código de Lambda. Para ver una lista de los tiempos de ejecución admitidos para cada tipo de análisis, consulte Tiempos de ejecución admitidos: análisis estándar de Lambda con Amazon Inspector y Tiempos de ejecución admitidos: análisis de código de Lambda con Amazon Inspector.

Además de contar con un tiempo de ejecución admitido, una función de Lambda necesita cumplir los siguientes criterios para que sea elegible para los análisis de Amazon Inspector.

- La función se ha invocado o actualizado en los últimos 90 días.
- La función está marcada con `$LATEST`.
- La función no se ha excluido de los análisis con etiquetas.

> **Note**
>
> Las funciones de Lambda que no se hayan invocado o modificado en los últimos 90 días se excluyen automáticamente de los análisis. Amazon Inspector reanuda el análisis de una función excluida automáticamente si se invoca de nuevo o si se realizan cambios en el código de la función de Lambda.

Análisis estándar de Lambda con Amazon Inspector

El análisis estándar de Lambda con Amazon Inspector identifica las vulnerabilidades de software en las dependencias de los paquetes de la aplicación que añade a las capas y el código de una función de Lambda. Por ejemplo, si la función de Lambda utiliza una versión del paquete `python-jwt` que incluye una vulnerabilidad conocida, el análisis estándar de Lambda generará un hallazgo para esa función.

Si Amazon Inspector detecta una vulnerabilidad en las dependencias del paquete de la aplicación de la función de Lambda, Amazon Inspector genera un hallazgo detallado del tipo Vulnerabilidad de paquetes.

Para ver las instrucciones de activación de un tipo de análisis, consulte Activación de un tipo de análisis.

> **Note**
>
> El escaneo estándar de Lambda no analiza la dependencia del AWS SDK instalada de forma predeterminada en el entorno de ejecución de Lambda. Amazon Inspector solo explora las dependencias cargadas con el código de función o heredadas de una capa.

> **Note**
>
> Al desactivar el análisis estándar de Lambda con Amazon Inspector, también se desactiva el análisis de código de Lambda con Amazon Inspector.

Exclusión de funciones del análisis estándar de Lambda

Puede etiquetar determinadas funciones para excluirlas del análisis estándar de Lambda con Amazon Inspector. Excluir funciones de los análisis ayuda a evitar recibir alertas no procesables.

Para excluir una función de Lambda del análisis estándar de Lambda, etiquete la función con el siguiente par de clave y valor:

- Clave: `InspectorExclusion`
- Valor: `LambdaStandardScanning`

Exclusión de una función del análisis estándar de Lambda

1. Abra la consola en https://console.aws.amazon.com/lambda/.
2. Seleccione Funciones.
3. En la tabla de funciones, seleccione el nombre de una función que querría excluir del análisis estándar de Lambda con Amazon Inspector.
4. Seleccione Configuración y elija Etiquetas en el menú.

5. Seleccione Administrar etiquetas y, a continuación, Agregar nueva etiqueta.
6. En el campo Clave, escriba `InspectorExclusion` y, en el campo Valor, escriba `LambdaStandardScanning`.
7. Seleccione Guardar para agregar la etiqueta y excluir la función del análisis estándar de Lambda con Amazon Inspector.

Para obtener más información sobre cómo agregar etiquetas en Lambda, consulte Uso de etiquetas en funciones de Lambda.

Análisis de código de Lambda con Amazon Inspector

> **Important**
>
> El análisis de código captura fragmentos de código de las funciones de Lambda para resaltar las vulnerabilidades detectadas. Estos fragmentos pueden contener credenciales codificadas u otros tipos de información confidencial en formato de texto no cifrado.

El escaneo de código Lambda de Amazon Inspector analiza el código de la aplicación personalizada dentro de una función de Lambda para detectar vulnerabilidades en el código según AWS las prácticas recomendadas de seguridad. El análisis de código de Lambda puede detectar fallos de inyección, fugas de datos, errores de criptografía débil o una falta de cifrado en el código. Para obtener información acerca de las regiones donde está disponible, consulte Disponibilidad de características específicas por región.

El análisis estándar de Lambda es una característica que evalúa las dependencias de paquetes de la aplicación empleadas en una función en busca de vulnerabilidades y riesgos comunes (CVE). Puede activar el análisis de código de Lambda junto al análisis estándar de Lambda.

Amazon Inspector evalúa el código de la aplicación de la función de Lambda mediante razonamiento automatizado y machine learning de conformidad con los estándares generales de seguridad. Identifica las infracciones y vulnerabilidades de las políticas basándose en detectores internos desarrollados en colaboración con Amazon CodeGuru. Para obtener una lista de posibles detecciones, consulte la biblioteca de CodeGuru detectores.

Si Amazon Inspector detecta una vulnerabilidad en el código de la aplicación de la función de Lambda, Amazon Inspector genera un hallazgo detallado del tipo Vulnerabilidad de código. En este

tipo de resultado se incluye la ubicación exacta del problema en el código, un fragmento de código en el que se muestra el problema y una sugerencia de corrección. La solución sugerida incluye bloques de plug-and-play código que puede usar para reemplazar las líneas de código vulnerables. Para ese resultado, se proporcionan estas correcciones de código sugeridas, además de una guía general de corrección de código.

> **Important**
>
> Las sugerencias de corrección de código se basan en el razonamiento automatizado y los servicios de IA generativa y, por lo tanto, es posible que no funcionen según lo previsto. El usuario se hace responsable de las sugerencias de corrección de código que adopte. Revise las sugerencias de corrección de código antes de adoptarlas. Es posible que deba modificar dichas sugerencias para garantizar que el código lleve a cabo las acciones previstas. Consulte la Política de IA responsable.

Cifrado del código en los hallazgos de vulnerabilidades de código

El servicio almacena los fragmentos de código detectados en relación con una vulnerabilidad de código detectada mediante el escaneo de código Lambda. CodeGuru De forma predeterminada, CodeGuru se utiliza una AWS clave propia controlada por para cifrar el código; sin embargo, puede utilizar su propia clave gestionada por el cliente para el cifrado a través de la API de Amazon Inspector. Para obtener más información, consulte Cifrado de código en reposo en los hallazgos

Puede activar el análisis de código de Lambda junto al análisis estándar de Lambda. Para ver las instrucciones de activación de un tipo de análisis, consulte Activación de un tipo de análisis.

Exclusión de funciones del análisis de código de Lambda

Puede etiquetar determinadas funciones para excluirlas del análisis de código de Lambda con Amazon Inspector. Excluir funciones de los análisis ayuda a evitar recibir alertas no procesables.

Para excluir una función de Lambda de los análisis de código de Lambda con Amazon Inspector, etiquete la función con el siguiente par de clave y valor:

- Clave: `InspectorCodeExclusion`
- Valor: `LambdaCodeScanning`

Exclusión de una función del análisis de código de Lambda

1. Inicie sesión en la consola de Lambda en https://console.aws.amazon.com/lambda/.
2. Seleccione Funciones.
3. En la tabla de funciones, seleccione el nombre de una función que querría excluir del análisis de código de Lambda con Amazon Inspector.
4. Seleccione Configuración y elija Etiquetas en el menú.
5. Seleccione Administrar etiquetas y, a continuación, Agregar nueva etiqueta.
6. En el campo Clave, escriba `InspectorCodeExclusion` y, en el campo Valor, escriba `LambdaCodeScanning`.
7. Seleccione Guardar para agregar la etiqueta y excluir la función del análisis de código de Lambda con Amazon Inspector.

Para obtener más información sobre cómo agregar etiquetas en Lambda, consulte Uso de etiquetas en funciones de Lambda.

Desactivación de un tipo de análisis

Puede desactivar un nuevo tipo de análisis de Amazon Inspector en cualquier momento. Al desactivar un tipo de análisis, se pierde acceso a todos los hallazgos de la cuenta generados por análisis de este tipo. Si se vuelve a activar el tipo de análisis, se analizan los recursos elegibles y Amazon Inspector genera nuevos hallazgos. Si desea mantener un registro con todos los datos de los hallazgos, exporte los hallazgos antes de desactivar un tipo de análisis. Para obtener más información, consulte Exportación de informes de hallazgos de Amazon Inspector.

Al desactivar un tipo de escaneo, pueden producirse ciertos cambios en esa AWS cuenta en función del tipo de escaneo que se desactive. A continuación se indican los cambios que se producirán si desactiva los siguientes tipos de análisis:

- Análisis de Amazon EC2: al desactivar los análisis de Amazon EC2 con Amazon Inspector en una cuenta, se eliminan las siguientes asociaciones de SSM que utiliza Amazon Inspector.
  - `InspectorDistributor-do-not-delete`
  - `InspectorInventoryCollection-do-not-delete`
  - `InspectorLinuxDistributor-do-not-delete`
  - `InvokeInspectorLinuxSsmPlugin-do-not-delete`

  - `InvokeInspectorSsmPlugin-do-not-delete`. Además, el complemento SSM de Amazon Inspector instalado a través de esta asociación se elimina de todos sus Windows hosts. Para obtener más información, consulte Análisis de instancias de Windows.
- Análisis de Amazon ECR: cuando desactiva los análisis de imágenes de contenedores de Amazon ECR en una cuenta, el tipo de análisis de Amazon ECR de la cuenta cambia de Análisis mejorado con Amazon ECR a Análisis básico con Amazon ECR.
- Análisis estándar de Lambda: al desactivar los análisis estándar de Lambda en una cuenta, se desactiva el análisis de código de Lambda si este estaba activo. Además, se elimina el canal vinculado al CloudTrail servicio que se creó cuando se activó el escaneo.

Desactivación de análisis

Cuando se desactivan todos los tipos de análisis en una cuenta, también se desactiva Amazon Inspector dicha cuenta de la Región de AWS correspondiente. Para obtener más información, consulte Desactivación de Amazon Inspector.

Si desea completar este procedimiento en un entorno de varias cuentas, complete los siguientes pasos con la sesión iniciada como administrador delegado de Amazon Inspector.

Console

Desactivación de análisis

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee desactivar los escaneos.
3. En el panel de navegación, elija Administración de cuentas.
4. Elija la pestaña Cuentas para ver el estado de los análisis de una cuenta.
5. Marque la casilla correspondiente a cada cuenta para la que desee desactivar los análisis.
6. Elija Acciones y, entre las opciones de Desactivar, seleccione el tipo de análisis que quiere desactivar.
7. (Recomendado) Repita estos pasos en cada uno de los tipos de escaneo en Región de AWS los que desee desactivar ese tipo de escaneo.

API

Ejecute la operación de la API Disable. En la solicitud, proporcione los ID de las cuentas en las que desea desactivar los análisis y, para `resourceTypes`, proporcione uno o más valores entre `EC2`, `ECR`, `LAMBDA` y `LAMBDA_CODE` para desactivar los análisis.

El Center for Internet Security (CIS) busca instancias EC2

Cuando habilita el escaneo EC2 de Amazon Inspector para una cuenta, permite a Amazon Inspector realizar o programar escaneos CIS. Los escaneos CIS de Amazon Inspector comparan los sistemas operativos de sus instancias de Amazon EC2 para comprobar si están configurados de acuerdo con las recomendaciones de mejores prácticas establecidas por el Center for Internet Security. El programa CIS Security Benchmarks proporciona las bases de configuración estándar del sector y las mejores prácticas para configurar un sistema de forma segura. Para obtener más información, consulte ¿Qué son los puntos de referencia de CIS?

Amazon Inspector realiza escaneos CIS en las instancias Amazon EC2 de destino en función de las etiquetas de instancia y el programa de escaneo que defina en una configuración de escaneo. Para cada instancia de destino, Amazon Inspector realiza una serie de comprobaciones en la instancia. Cada comprobación evalúa si la configuración del sistema cumple con una recomendación específica del CIS Benchmark. Cada verificación tiene un identificador y un título de verificación de CIS, que se correlacionan directamente con una recomendación de CIS Benchmark para esa plataforma. Cuando se complete un análisis, podrá ver los resultados y ver qué comprobaciones para ese sistema su instancia ha superado, ha fallado o ha omitido.

Requisitos de instancia EC2 para escaneos CIS de Amazon Inspector

Para ejecutar un escaneo CIS en la instancia, Amazon Inspector requiere que la instancia cumpla los siguientes criterios:

- El sistema operativo de la instancia es uno de los sistemas operativos compatibles con los escaneos CIS. Para ver una lista completa de los sistemas operativos admitidos, consulte Sistemas operativos compatibles: escaneo CIS.
- La instancia es una instancia gestionada por Amazon EC2 Systems Manager (SSM). Para obtener más información, consulte Uso del agente de SSM.
- La instancia tiene instalado el complemento Amazon Inspector SSM. Amazon Inspector instala automáticamente este complemento para las instancias gestionadas por SSM.
- La instancia tiene un perfil de instancia que concede permisos a SSM para gestionar la instancia y a Amazon Inspector para ejecutar escaneos de CIS para esa instancia. Para conceder estos permisos, asocie las ManagedCispolicy políticas AmazonInspector2FullAccess, AmazonSSM ManagedInstanceCore y AmazonInspector2 a un rol de IAM y asocie ese rol a su instancia

como un perfil de instancia. Para obtener instrucciones sobre cómo crear y adjuntar un perfil de instancia, consulte Trabajar con funciones de IAM en la Guía del usuario de Amazon EC2.

> **Note**
>
> Habilitar la inspección profunda de Amazon Inspector ya no es un requisito cuando se ejecuta un escaneo CIS en una instancia. Si inhabilitas la inspección profunda, Amazon Inspector seguirá instalando el agente SSM, pero ya no se invocará el complemento para ejecutar la inspección profunda. Esto significa que la siguiente asociación estará presente en su cuenta:`InspectorLinuxDistributor-do-not-delete`.

Ejecutando escaneos CIS

Puede ejecutar un escaneo CIS una vez bajo demanda o como un escaneo periódico programado. Para ejecutar un escaneo, primero debe crear una configuración de escaneo.

Al crear una configuración de escaneo, se especifican los pares clave-valor de etiquetas para usarlos en las instancias de destino. Si es el administrador delegado de Amazon Inspector de una organización, puede especificar varias cuentas en la configuración de escaneo y Amazon Inspector buscará instancias con las etiquetas especificadas en cada una de esas cuentas. Usted elige el nivel de referencia CIS para el escaneo. Para cada punto de referencia, CIS admite un perfil de nivel 1 y nivel 2 diseñado para proporcionar puntos de referencia para los diferentes niveles de seguridad que puedan requerir los diferentes entornos.

- Nivel 1: recomienda los ajustes de seguridad básicos esenciales que se pueden configurar en cualquier sistema. La implementación de estos ajustes debería provocar una interrupción mínima o nula del servicio. El objetivo de estas recomendaciones es reducir la cantidad de puntos de entrada a sus sistemas, reduciendo así los riesgos generales de ciberseguridad.
- Nivel 2: recomienda configuraciones de seguridad más avanzadas para entornos de alta seguridad. La implementación de estos ajustes requiere planificación y coordinación para minimizar el riesgo de impacto empresarial. El objetivo de estas recomendaciones es ayudarlo a lograr el cumplimiento normativo.

El nivel 2 amplía el nivel 1. Al elegir el nivel 2, Amazon Inspector comprueba todas las configuraciones recomendadas para los niveles 1 y 2.

Tras definir los parámetros del análisis, puede elegir si desea ejecutarlo como un análisis único, que se ejecuta después de completar la configuración, o como un análisis periódico. Los escaneos periódicos se pueden realizar de forma diaria, semanal o mensual, en el momento que prefiera.

> **Tip**
>
> Le recomendamos que elija el día y la hora que tengan menos probabilidades de afectar al sistema mientras se esté realizando el análisis.

Para crear una configuración de escaneo CIS

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione el Región de AWS lugar en el que desee ejecutar el escaneo CIS.
3. En el panel de navegación, en Escaneos bajo demanda, seleccione Escaneos CIS.
4. Seleccione Crear nueva digitalización.
    a. Introduzca un nombre de configuración de escaneo.
    b. En el recurso Target, introduzca la clave y el valor correspondiente de una etiqueta en las instancias que desee escanear. Puede especificar un total de 25 etiquetas para incluirlas en el escaneo y, para cada clave, puede especificar hasta cinco valores diferentes.
    c. Elija un nivel de referencia CIS. Puede seleccionar el nivel 1 para las configuraciones de seguridad básicas o el nivel 2 para las configuraciones de seguridad avanzadas.
5. En el caso de las cuentas de Target, especifique qué cuentas desea incluir en el análisis. Una cuenta independiente o un miembro de una organización pueden seleccionar Self para crear una configuración de escaneo para su cuenta. Un administrador delegado de Amazon Inspector puede seleccionar Todas las cuentas para orientarse a todas las cuentas de la organización o seleccionar Especificar cuentas y especificar un subconjunto de cuentas de miembros a las que dirigirse. El administrador delegado puede introducir, `SELF` en lugar de un identificador de cuenta, un identificador para crear una configuración de digitalización para su propia cuenta. Para más información, consulte Consideraciones para gestionar los escaneos CIS de Amazon Inspector en una AWS organización.
6. Elija una programación para los escaneos. Elija entre un escaneo único, que se ejecutará tan pronto como termine de crear la configuración de escaneo, o un escaneo periódico, que se ejecutará a la hora programada que elija hasta que se elimine.

7. Seleccione Crear para terminar de crear la configuración de digitalización.

Visualización y edición de las configuraciones de escaneo CIS

Puede ver o editar los escaneos previamente programados en cualquier momento.

Para ver o editar la configuración de un escaneo CIS

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione el Región de AWS lugar donde creó la configuración de escaneo CIS.
3. En el panel de navegación, en Escaneos bajo demanda, seleccione Escaneos CIS.
4. Seleccione Programado para ver las configuraciones de escaneo programadas.
5. Seleccione un elemento de la columna del nombre de la configuración de escaneo para abrir los detalles de esa configuración de escaneo.
6. (Opcional) Seleccione Editar para cambiar los parámetros de este escaneo.

Visualización de los resultados de sus escaneos CIS

Amazon Inspector crea un trabajo de escaneo cada vez que se ejecuta una configuración de escaneo y recopila los resultados del escaneo con un ID de escaneo único.

Los resultados del escaneo están disponibles durante 90 días después de que se complete el escaneo. Puede ver los resultados del escaneo agregados por cheque o por recurso de destino.

Los resultados del escaneo se agregan por comprobaciones

Los resultados del escaneo se agrupan por cada comprobación individual realizada durante el escaneo. Para cada comprobación, recibirá un informe del número de recursos aprobados, fallidos o omitidos.

Los resultados del escaneo se agregan por recurso

Los resultados del análisis se agrupan por cada recurso al que se dirigió la configuración del análisis. Para cada recurso, se obtiene un informe en el que se comprueba que un recurso ha superado, ha fallado o se ha omitido en relación con ese recurso.

Para ver los resultados del análisis

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione el Región de AWS lugar en el que desee ver los resultados del escaneo.
3. En el panel de navegación, en Escaneos bajo demanda, seleccione Escaneos CIS.
4. Seleccione el ID del escaneado cuyos resultados desee ver en la columna Scan ID.
5. Elija cómo desea ver los resultados del escaneo:
    - Seleccione la pestaña Comprobaciones para ver los resultados del escaneo agregados por comprobaciones.
        - Para una comprobación de la lista, seleccione un número entre las opciones aprobadas, omitidas o rechazadas en la columna Estado del recurso para abrir una vista de los recursos filtrados por ese estado y esa comprobación.
    - Seleccione la pestaña Recursos escaneados para ver los resultados del escaneo agregados por recurso.
        - Seleccione un recurso para abrir un panel de detalles en el que se enumeran las comprobaciones que el recurso ha superado, fallado u omitido.
6. (Opcional) Usa la barra de filtros en cualquiera de las vistas para refinar los resultados.

Puede descargar los resultados de un análisis CIS mediante la consola o la API.

Para descargar los resultados del escaneo

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione el Región de AWS lugar en el que desee ver los resultados del escaneo.
3. En el panel de navegación, en Escaneos bajo demanda, seleccione Escaneos CIS.
4. Seleccione el ID del escaneado cuyos resultados desee ver en la columna Scan ID.
5. Elija Descargar. Si es el administrador delegado, puede optar por descargar los resultados de cuentas de miembros específicas.

Consideraciones para gestionar los escaneos CIS de Amazon Inspector en una AWS organización

Al ejecutar escaneos de CIS en una organización, las cuentas de los miembros y los administradores delegados de Amazon Inspector interactúan con las configuraciones de escaneo de CIS y los resultados de los escaneos de diferentes maneras.

Cuando un administrador delegado crea una configuración de escaneo CIS para todas las cuentas o una lista de identificadores de cuentas de miembros, la organización es propietaria de esa configuración de escaneo. Sea cual sea la cuenta, el administrador delegado actual puede administrar las configuraciones de escaneo que sean propiedad de la organización, incluso si las creó una cuenta diferente. Las configuraciones de escaneo CIS propiedad de la organización tendrán un ARN que indique el ID de la organización como propietario, siguiendo el patrón:. `arn:aws:inspector2:`*`Region`*`:`*`111122223333`*`:owner/`*`OrganizationId`*`/cis-configuration/`*`scanId`* El ID de la cuenta será el ID de la cuenta de administración de Organizations.

> **Important**
>
> No puede añadir etiquetas a las configuraciones de escaneo CIS que sean propiedad de la organización.

Cuando un administrador delegado crea una configuración de digitalización y la especifica `SELF` como cuenta de destino, su cuenta es la propietaria de esa configuración de digitalización. Incluso si abandonan su organización, pueden seguir gestionando esa configuración de digitalización.

> **Note**
>
> Un administrador delegado no puede cambiar los objetivos de una configuración de escaneo que tenga como objetivo`SELF`.

Las configuraciones de escaneo creadas por las cuentas de los miembros, las cuentas independientes o los administradores delegados con el objetivo `SELF` como destino son propiedad de la cuenta que las creó. Estas configuraciones de escaneo CIS tienen un ARN que indica esa cuenta como propietaria siguiendo el patrón:.

`arn:aws:inspector2:Region:111122223333:owner/111122223333/cis-configuration/scanId` El ID de la cuenta será la cuenta que creó el escaneo.

La cuenta de un miembro de una organización puede crear configuraciones de escaneo para su propia cuenta. El administrador delegado puede ver las configuraciones de digitalización creadas por los miembros, pero no puede editarlas ni eliminarlas. Si la cuenta de un miembro abandona la organización, el administrador delegado ya no podrá ver las configuraciones de digitalización creadas por esa cuenta.

El administrador delegado puede ver los resultados del escaneo de cualquier cuenta de la organización, incluidas las programadas por los miembros. La cuenta de un miembro puede ver los resultados de cualquier análisis realizado por el CIS para detectar los recursos de su cuenta, incluidos los programados por el administrador delegado.

Depósitos de Amazon S3 propiedad de Amazon Inspector que se utilizan para los escaneos CIS de Amazon Inspector

Amazon Inspector prepara los archivos de definición actualizados del Lenguaje Abierto de Evaluación y Vulnerabilidad (OVAL) necesarios para los escaneos del CIS. En la siguiente tabla se enumeran todos los buckets de Amazon S3 propiedad de Amazon Inspector con definiciones OVAL que CIS scan utiliza según las admitidas. Región de AWS Si es necesario, los cubos deberían figurar en la lista de permitidos en las VPC.

> **Note**
>
> Los detalles de cada uno de los siguientes depósitos de Amazon S3 propiedad de Amazon Inspector no están sujetos a cambios. Sin embargo, es posible que la lista se actualice para incluir las nuevas Regiones de AWS ofertas de soporte. No puede usar estos buckets para otras operaciones de Amazon S3 ni en sus propios buckets de Amazon S3.

Cubo CIS	Región de AWS
`cis-datasets-prod-arn-5908f6f`	Europa (Estocolmo)
`cis-datasets-prod-bah-8f88801`	Medio Oriente (Baréin)
`cis-datasets-prod-bjs-0f40506`	China (Pekín)

Cubo CIS	Región de AWS
`cis-datasets-prod-bom-435a167`	Asia-Pacífico (Bombay)
`cis-datasets-prod-cdg-f3a9c58`	Europa (París)
`cis-datasets-prod-cgk-09eb12f`	Asia-Pacífico (Yakarta)
`cis-datasets-prod-cmh-63030b9`	Este de EE. UU. (Ohio)
`cis-datasets-prod-cpt-02c5c6f`	África (Ciudad del Cabo)
`cis-datasets-prod-dub-984936f`	Europa (Irlanda)
`cis-datasets-prod-fra-6eb96eb`	Europa (Fráncfort)
`cis-datasets-prod-gru-de69f99`	América del Sur (São Paulo)
`cis-datasets-prod-hkg-8e30800`	Asia-Pacífico (Hong Kong)
`cis-datasets-prod-iad-8438411`	Este de EE. UU. (Norte de Virginia)
`cis-datasets-prod-icn-f4eff1c`	Asia-Pacífico (Seúl)
`cis-datasets-prod-kix-5743b21`	Asia-Pacífico (Osaka)
`cis-datasets-prod-lhr-8b1fbd0`	Europa (Londres)
`cis-datasets-prod-mxp-7b1bbce`	Europa (Milán)
`cis-datasets-prod-nrt-464f684`	Asia-Pacífico (Tokio)
`cis-datasets-prod-osu-5bead6f`	AWS GovCloud (Este de EE. UU.)
`cis-datasets-prod-pdt-adadf9c`	AWS GovCloud (Estados Unidos-Oeste)
`cis-datasets-prod-pdx-acfb052`	Oeste de EE. UU. (Oregón)
`cis-datasets-prod-sfo-1515ba8`	Oeste de EE. UU. (Norte de California)
`cis-datasets-prod-sin-309725b`	Asia-Pacífico (Singapur)

Cubo CIS	Región de AWS
`cis-datasets-prod-syd-f349107`	Asia-Pacífico (Sídney)
`cis-datasets-prod-yul-5e0c95e`	Canadá (centro)
`cis-datasets-prod-zhy-5a8eacb`	China (Ningxia)
`cis-datasets-prod-zrh-67e0e3d`	Europa (Zúrich)

Evaluación de la cobertura de Amazon Inspector para el entorno de AWS

Con el fin de ayudarle a evaluar e interpretar la cobertura de Amazon Inspector de su entorno de AWS, la página Administración de cuentas de la consola de Amazon Inspector proporciona estadísticas y detalles acerca del estado del análisis de cuentas y recursos de Amazon Inspector. En esta página, puede revisar estadísticas agregadas y otros datos relacionados con sus recursos. También puede realizar un análisis exhaustivo de la cobertura de Amazon Inspector para recursos concretos y desglosar los detalles de ciertos recursos para revisar los hallazgos. Si es administrador delegado de Amazon Inspector de una organización, entre los datos se incluyen estadísticas y detalles de todas las cuentas de la organización.

Evaluación de la cobertura de Amazon Inspector para el entorno de AWS

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. En el panel de navegación, elija Administración de cuentas.
3. En la página Administración de cuentas, elija una de las cinco pestañas de vistas de cobertura disponibles:

   - Cuentas, para ver la cobertura a nivel de cuenta
   - Instancias, para ver la cobertura de instancias de Amazon Elastic Compute Cloud (Amazon EC2)
   - Repositorios, para ver la cobertura de repositorios de Amazon Elastic Container Registry (Amazon ECR)
   - Imágenes, para ver la cobertura de imágenes de contenedores de Amazon ECR
   - Lambda, para ver la cobertura de funciones de Lambda

En los temas de esta sección se describe la información que proporciona cada pestaña, así como el estado del análisis que puede tener cada recurso.

Temas

- Evaluación de la cobertura de imágenes de contenedores de Amazon ECR
- Evaluación de la cobertura de las funciones de AWS Lambda

Evaluación de la cobertura a nivel de cuenta

Si su cuenta no forma parte de una organización o no es la cuenta de administrador delegado de Amazon Inspector de una organización, la pestaña Cuentas proporciona información acerca de la cuenta y el estado del análisis de recursos de la cuenta. En esta pestaña, puede activar o desactivar los análisis para todos los tipos de recursos de la cuenta o solo para algunos. Para obtener más información, consulte Análisis automatizado de recursos con Amazon Inspector.

Si su cuenta es la cuenta de administrador delegado de Amazon Inspector de una organización, la pestaña Cuentas proporciona la configuración de activación automática de las cuentas de la organización y enumera todas las cuentas de la organización. Para cada cuenta, en la lista se indica si Amazon Inspector está activado en la cuenta y, si lo está, los tipos de análisis de recursos activados en la cuenta. Como administrador delegado, puede utilizar esta pestaña para modificar la configuración de activación automática de la organización. También puede activar o desactivar tipos de análisis de recursos específicos de algunas cuentas de miembros. Para obtener más información, consulte Activación de los análisis de Amazon Inspector para cuentas de miembros.

Evaluación de la cobertura de instancias de Amazon EC2

En la pestaña Instancias, se muestran las instancias de Amazon EC2 del entorno de AWS. Las listas se agrupan en las siguientes pestañas:

- Todos: muestra todas las instancias del entorno. En la columna Estado, se indica el estado de análisis actual de una instancia.
- Analizar: muestra todas las instancias que Amazon Inspector supervisa y analiza activamente en el entorno.
- Sin analizar: muestra todas las instancias que Amazon Inspector no supervisa y analiza activamente en el entorno. En la columna Motivo, se indica por qué Amazon Inspector no supervisa y analiza una instancia.

  Una instancia de EC2 puede aparecer en la pestaña Sin analizar por muchos motivos. Amazon Inspector utiliza AWS Systems Manager (SSM) y el agente de SSM para supervisar y analizar automáticamente las instancias de EC3 en busca de vulnerabilidades. Si en una instancia no se

está ejecutando el agente de SSM, no tiene el rol de AWS Identity and Access Management (IAM) que admite Systems Manager o está ejecutando un sistema operativo o arquitectura compatible, Amazon Inspector no puede supervisar y analizar la instancia. Para obtener más información, consulte Análisis de instancias de Amazon EC2.

En cada pestaña, la columna Cuenta especifica la Cuenta de AWS propietaria de una instancia.

Etiquetas de instancias de EC2: esta columna muestra las etiquetas asociadas a la instancia y se puede utilizar para determinar si la instancia se han excluido de los análisis mediante etiquetas.

Sistema operativo: en esta columna se muestra el tipo de sistema operativo, que puede ser `WINDOWS`, `MAC`, `LINUX` o `UNKNOWN`.

Uso supervisado: en esta columna se muestra si Amazon Inspector utiliza el método de análisisbasado en agentes o sin agente en esta instancia.

Último análisis: en esta columna se muestra la última vez que Amazon Inspector comprobó el recurso en busca de vulnerabilidades. La frecuencia con la que Amazon Inspector realiza análisis depende del método que utilice para analizar la instancia.

Para revisar detalles adicionales acerca de una instancia de EC2, siga el enlace de la columna Instancia de EC2. A continuación, Amazon Inspector muestra los detalles sobre la instancia y los hallazgos de esta. Para revisar los detalles de un hallazgo, siga el enlace de la columna Título. Para obtener información acerca de estos detalles, consulte Detalles de los hallazgos de Amazon Inspector.

Valores de estado de escaneo para instancias de Amazon EC2

En el caso de las instancias de Amazon Elastic Compute Cloud (Amazon EC2), los valores de Estado posibles son los siguientes:

- Supervisión activa: Amazon Inspector supervisa y analiza continuamente la instancia.
- Instancia de EC2 detenida: Amazon Inspector ha detenido el análisis de la instancia porque se ha detenido la instancia. Los hallazgos se mantendrán hasta que se finalice la instancia. Si se reinicia la instancia, Amazon Inspector reanudará automáticamente el análisis de la instancia.
- Error interno: se ha producido un error interno cuando Amazon Inspector ha intentado analizar la instancia. Amazon Inspector solucionará automáticamente el error y reanudará el análisis lo antes posible.

- Sin inventario: Amazon Inspector no ha encontrado el inventario de aplicaciones de software necesario para analizar la instancia. Es posible que las asociaciones de Amazon Inspector relacionadas con la instancia se hayan eliminado o que no se hayan ejecutado correctamente.

  Para corregir este problema, utilice AWS Systems Manager, que comprobará si la asociación `InspectorInventoryCollection-do-not-delete` existe y si el estado de la asociación es correcto. También puede utilizar AWS Systems Manager Fleet Manager para verificar el inventario de aplicaciones de software de la instancia.
- Pendiente desactivado: Amazon Inspector ha dejado de analizar la instancia. La instancia se está deshabilitando, pendiente de la finalización de tareas de limpieza.
- Pendiente de análisis inicial: Amazon Inspector ha añadido la instancia a la cola para realizar un análisis inicial.
- Recurso finalizado: la instancia ha finalizado. Amazon Inspector está limpiando los hallazgos existentes y los datos de cobertura de la instancia.
- Inventario obsoleto: Amazon Inspector no ha podido recopilar un inventario de aplicaciones de software actualizado para la instancia que se haya capturado durante los últimos siete días.

  Para corregir este problema, utilice AWS Systems Manager, que comprobará si las asociaciones de Amazon Inspector necesarias existen y si están ejecutando la instancia. También puede utilizar AWS Systems Manager Fleet Manager para verificar el inventario de aplicaciones de software de la instancia.
- Instancia de EC2 no administrada: Amazon Inspector no está supervisando ni analizando la instancia. AWS Systems Manager no administra la instancia.

  Para solucionar este problema, puede utilizar el AWSSupport-TroubleshootManagedInstance runbook proporcionado por AWS Systems Manager Automation. Una vez que haya configurado AWS Systems Manager para administrar la instancia, Amazon Inspector comenzará al instante a supervisar y a analizar continuamente la instancia.
- SO no compatible Amazon Inspector no supervisa ni analiza la instancia. La instancia utiliza un sistema operativo o una arquitectura no compatible con Amazon Inspector. Para obtener información sobre los sistemas operativos compatibles con Amazon Inspector, consulte Sistemas operativos admitidos para el análisis de Amazon EC2.
- Supervisión activa con errores parciales: si se muestra este estado, significa que el análisis de EC2 está activado, aunque hay errores relacionados con la Inspección exhaustiva de Amazon Inspector para instancias de Linux de Amazon EC2. Los posibles errores en las inspecciones profundas son:

- Se ha superado el límite de recogida de paquetes con inspección exhaustiva: la instancia ha superado el límite de 5000 paquetes para la inspección exhaustiva de Amazon Inspector. Para reanudar la inspección exhaustiva en este caso, puede intentar ajustar las rutas personalizadas asociadas a la cuenta.
- Se ha superado el límite de inventario de SSM diario de inspección exhaustiva: el agente de SSM no ha podido enviar el inventario a Amazon Inspector porque ya se ha alcanzado la cuota de SSM de datos de inventario recopilados por instancia y día para esta instancia. Para obtener más información, consulte Puntos de conexión y cuotas de Amazon EC2 Systems Manager.
- Se ha superado el límite de tiempo de recogida por inspección exhaustiva: Amazon Inspector no ha podido extraer el inventario del paquete porque el tiempo de recogida del paquete ha superado el límite máximo de 15 minutos.
- La inspección profunda no tiene inventario: el complemento de SSM de Amazon Inspector todavía no ha recopilado un inventario de paquetes para esta instancia. Suele pasar porque hay un análisis pendiente. No obstante, si el estado persiste durante 6 horas, utilice Amazon EC2 Systems Manager, que comprobará si las asociaciones de Amazon Inspector necesarias existen y si se están ejecutando para la instancia.

Para obtener información acerca de la configuración de análisis para una instancia de EC2, consulte Análisis de instancias de Amazon EC2.

Evaluación de la cobertura de repositorios de Amazon ECR

En la pestaña Repositorios se muestran los repositorios de Amazon ECR en su entorno de AWS. Las listas se agrupan en las siguientes pestañas:

- Todos: muestra todos los repositorios del entorno. En la columna Estado, se indica el estado de análisis actual de un repositorio.
- Activado: muestra todos los repositorios del entorno en los que se ha configurado Amazon Inspector para supervisarlos y analizarlos. En la columna Estado, se indica el estado de análisis actual de un repositorio.
- No activado: muestra todos los repositorios del entorno que Amazon Inspector no está supervisando ni analizando. En la columna Motivo, se indica por qué Amazon Inspector no supervisa y analiza un repositorio.

En cada pestaña, la columna Cuenta especifica la Cuenta de AWS propietaria de un repositorio.

Para revisar detalles adicionales acerca de un repositorio, elija el nombre de un repositorio. A continuación, Amazon Inspector muestra una lista de las imágenes de contenedores del repositorio y detalles de cada imagen. Algunos de los detalles que se muestran son la etiqueta de la imagen, un resumen de la imagen y el estado de análisis. También se incluyen estadísticas importantes sobre hallazgos como, por ejemplo, el número de hallazgos críticos de la imagen. Para revisar detenidamente los datos de soporte relacionados con estadísticas de hallazgos, elija la etiqueta de una imagen.

Escaneando valores de estado para los repositorios de Amazon ECR

Para un repositorio de Amazon Elastic Container Registry (Amazon ECR), los valores de estado posibles son:

- Activado (continuo): en el caso de un repositorio, Amazon Inspector supervisa continuamente las imágenes de este repositorio. Los análisis mejorados del repositorio se establecen en análisis continuo. Amazon Inspector escanea inicialmente las imágenes nuevas cuando se insertan y las vuelve a escanear si se publica un nuevo CVE relevante para esa imagen. Amazon Inspector seguirá supervisando las imágenes de este repositorio durante el tiempo de escaneo de ECR que configure.
- Activado (al pulsar): Amazon Inspector escanea automáticamente las imágenes de los contenedores individuales del repositorio cuando se inserta una nueva imagen. El escaneo mejorado se activa en el repositorio y se configura para que se escanee al insertarlo.
- Acceso denegado: Amazon Inspector no puede acceder al repositorio ni a ninguna de las imágenes de contenedores del repositorio.

  Para corregir este problema, compruebe que las políticas de AWS Identity and Access Management (IAM) del repositorio permitan a Amazon Inspector acceder al repositorio.
- Desactivado (manual): Amazon Inspector no supervisa ni analiza las imágenes de contenedor del repositorio. Los análisis de Amazon ECR del repositorio se establecen en análisis manuales y básicos.

  Para comenzar a analizar imágenes del repositorio con Amazon Inspector, establezca el parámetro de análisis del repositorio en análisis mejorado y, a continuación, elija si desea analizar las imágenes continuamente o solo cuando se inserte una nueva imagen.
- Activado (al pulsar): Amazon Inspector escanea automáticamente las imágenes de los contenedores individuales del repositorio cuando se inserta una nueva imagen. Los análisis mejorados del repositorio se establecen en analizar al enviar.

- Error interno: se produjo un error interno cuando Amazon Inspector intentó escanear el repositorio. Amazon Inspector solucionará automáticamente el error y reanudará el análisis lo antes posible.

Para obtener más información sobre la configuración de los ajustes de digitalización de los repositoriosAnálisis de imágenes de contenedores de Amazon ECR.

Evaluación de la cobertura de imágenes de contenedores de Amazon ECR

En la pestaña Imágenes se muestran las imágenes de contenedores de Amazon ECR del entorno de AWS. Las listas se agrupan en las siguientes pestañas:

- Todos: muestra todas las imágenes de contenedores del entorno. En la columna Estado, se indica el estado de análisis actual de una imagen.
- Analizar: muestra todas las imágenes de contenedores en las que se ha configurado Amazon Inspector para supervisarlas y analizarlas. En la columna Estado, se indica el estado de análisis actual de una imagen.
- Sin analizar: muestra todas las imágenes de contenedores que Amazon Inspector no supervisa y analiza en el entorno. En la columna Motivo, se indica por qué Amazon Inspector no supervisa y analiza una imagen.

  Una imagen de contenedor puede aparecer en la pestaña No activado por muchos motivos. Es posible que la imagen esté almacenada en un repositorio para el que no están activados los análisis de Amazon Inspector o que las reglas de filtrado de Amazon ECR eviten que el repositorio pueda analizarse. O bien, la imagen no se ha insertado o extraído en el número de días que configuró para volver a digitalizar el ECR. Para obtener más información, consulte Configuración de la duración de la redigitalización del ECR.

En cada pestaña, la columna Nombre del repositorio especifica el nombre del repositorio que almacena la imagen de contenedor. La columna Cuenta especifica la Cuenta de AWS propietaria del repositorio. En la columna Último análisis se muestra la última vez que Amazon Inspector comprobó el recurso en busca de vulnerabilidades. Estas comprobaciones pueden ser por motivo de una actualización de metadatos de los hallazgos, de una actualización del inventario de aplicaciones del recurso o de un análisis repetido en respuesta a una nueva lista de CVE. Para obtener más información, consulte Comportamientos de los análisis de Amazon ECR.

Si desea revisar detalles adicionales sobre una imagen de contenedor, siga el enlace de la columna Imagen de contenedor de ECR. A continuación, Amazon Inspector muestra los detalles sobre la imagen y los hallazgos de esta. Para revisar los detalles de un hallazgo, siga el enlace de la columna Título. Para obtener información acerca de estos detalles, consulte Detalles de los hallazgos de Amazon Inspector.

Valores de estado de digitalización para imágenes de contenedores de Amazon ECR

Para una imagen de contenedor de Amazon Elastic Container Registry, los valores de estado posibles son:

- Supervisión activa (continua): Amazon Inspector supervisa continuamente y la imagen y los nuevos escaneos se realizan en ella cada vez que se publica un nuevo CVE relevante. La duración del reescaneo de Amazon ECR de la imagen se actualiza cada vez que se empuja o se tira de la imagen. Los análisis mejorados están habilitados para el repositorio que almacena la imagen y se establecen en análisis continuo para el repositorio.
- Activado (al pulsar): Amazon Inspector escanea automáticamente la imagen cada vez que se inserta una nueva imagen. Los análisis mejorados están activados para el repositorio que almacena la imagen y se establecen en analizar al enviar para el repositorio.
- Error interno: se produjo un error interno cuando Amazon Inspector intentó escanear la imagen del contenedor. Amazon Inspector solucionará automáticamente el error y reanudará el análisis lo antes posible.
- Escaneo inicial pendiente: Amazon Inspector ha puesto la imagen en cola para un escaneo inicial.
- Los requisitos para el escaneo han caducado (continuo): Amazon Inspector suspendió el escaneo de la imagen. La imagen no se ha actualizado durante el período que ha especificado para los análisis repetidos y automatizados de imágenes en el repositorio. Puede empujar o tirar de la imagen para reanudar el escaneo.
- La capacidad de escaneo ha caducado (al pulsar): Amazon Inspector suspendió el escaneo de la imagen. La imagen no se ha actualizado durante el período que ha especificado para los análisis repetidos y automatizados de imágenes en el repositorio. Puede presionar la imagen para reanudar el escaneo.
- Analizar frecuencia de manera manual (manual): Amazon Inspector no analiza la imagen de contenedor de Amazon ECR. Los análisis de Amazon ECR del repositorio que almacena la imagen se establecen en análisis manuales y básicos. Para comenzar a analizar la imagen automáticamente con Amazon Inspector, establezca el parámetro del repositorio en análisis

mejorado y, a continuación, elija si desea analizar las imágenes continuamente o solo cuando se inserte una nueva imagen.

- Sistema operativo no compatible: Amazon Inspector no supervisa ni escanea la imagen. La imagen se basa en un sistema operativo no compatible con Amazon Inspector o utiliza un tipo de medio no compatible con Amazon Inspector.

  Para obtener información sobre los sistemas operativos compatibles con Amazon Inspector, consulte Sistemas operativos admitidos para el análisis de Amazon ECR. Para ver una lista de los tipos de medios compatibles con Amazon Inspector, consulte Tipos de medios compatibles.

Para obtener información acerca de la configuración de análisis para repositorios e imágenes, consulte Análisis de imágenes de contenedores de Amazon ECR.

Evaluación de la cobertura de las funciones de AWS Lambda

En la pestaña Lambda se muestran las funciones de Lambda del entorno de AWS. En esta página aparecen dos tablas: en la primera se muestran los detalles de cobertura de la función para el análisis estándar de Lambda, mientras que en la segunda se describe el análisis de código de Lambda. Las funciones se agrupan en las siguientes pestañas:

- Todos: muestra todas las funciones de Lambda del entorno. En la columna Estado, se indica el estado de análisis actual de una función de Lambda.
- Analizar: muestra las funciones de Lambda para las que se han configurado análisis de Amazon Inspector. En la columna Estado, se indica el estado de análisis actual de cada función de Lambda.
- Sin analizar: muestra las funciones de Lambda para las que no se han configurado análisis de Amazon Inspector. En la columna Motivo, se indica por qué Amazon Inspector no supervisa y analiza una función.

  Una función de Lambda puede aparecer en la pestaña Sin analizar por muchos motivos. Es posible que la función de Lambda pertenezca a una cuenta que no se ha añadido a Amazon Inspector o que las reglas de filtrado eviten que se pueda analizar la función. Para obtener más información, consulte AWS Lambda Funciones de escaneo.

En cada pestaña, la columna Nombre de la función especifica el nombre de la función de Lambda. La columna Cuenta especifica la Cuenta de AWS propietaria de la función. En Tiempo de ejecución, se

especifica el tiempo de ejecución de la función. En la columna Estado, se indica el estado de análisis actual de cada función de Lambda. En Etiquetas de recursos, se muestran las etiquetas que se han aplicado a la función. En la columna Último análisis se muestra la última vez que Amazon Inspector comprobó el recurso en busca de vulnerabilidades. Estas comprobaciones pueden ser por motivo de una actualización de metadatos de los hallazgos, de una actualización del inventario de aplicaciones del recurso o de un análisis repetido en respuesta a una nueva lista de CVE. Para obtener más información, consulte Comportamientos de los análisis de funciones de Lambda.

Escaneando valores de estado para funciones AWS Lambda

En el caso de una función de Lambda, los valores de Estado posibles son los siguientes:

- Supervisión activa: Amazon Inspector supervisa y analiza continuamente las funciones de Lambda. El análisis continuo incluye un análisis inicial de las nuevas funciones cuando se insertan en el repositorio y de los análisis repetidos y automatizados de funciones cuando se actualizan o cuando se publican nuevas listas de vulnerabilidades y riesgos comunes (CVE).
- Excluido por etiqueta: Amazon Inspector no analiza esta función porque se ha excluido de los análisis con etiquetas.
- La elegibilidad del análisis ha caducado: Amazon Inspector no supervisa esta función porque han transcurrido 90 días o más desde que se invocó o actualizó por última vez.
- Error interno: se ha producido un error interno cuando Amazon Inspector ha intentado analizar la función. Amazon Inspector solucionará automáticamente el error y reanudará el análisis lo antes posible.
- Pendiente de análisis inicial: Amazon Inspector ha añadido la función a la cola para realizar un análisis inicial.
- No compatible: la función de Lambda tiene un tiempo de ejecución no compatible.

Gestión de varias cuentas en Amazon Inspector with Organizations

Puede utilizar Amazon Inspector para gestionar varias cuentas asociadas a través de AWSOrganizations. Para gestionar varias cuentas de Amazon Inspector, la cuenta de gestión de Organizations designa una cuenta de la organización como cuenta de administrador delegado de Amazon Inspector. El administrador delegado administra Amazon Inspector para la organización y recibe permisos especiales para realizar tareas en nombre de su organización: Estas tareas incluyen activar o desactivar los escaneos de las cuentas de los miembros, ver los datos de búsqueda agregados de toda la organización y crear y administrar las reglas de supresión.

> **Note**
>
> Para habilitar Amazon Inspector mediante programación para varias cuentas en variasRegiones de AWS, puede utilizar un script shell desarrollado por Amazon Inspector. Para obtener más información sobre el uso de este script, consulte inspector2 - en el sitio web. enablement-with-cli GitHub

Temas

Comprensión de la relación entre la cuenta de administrador y las cuentas de miembros de Amazon Inspector

Cuando utiliza Amazon Inspector en un entorno con varias cuentas, la cuenta de administrador delegado de Amazon Inspector tiene acceso a ciertos metadatos. Estos metadatos incluyen los datos de configuración de Amazon EC2 y Amazon ECR y los resultados de los hallazgos de seguridad para cuentas de miembros. Asimismo, en la cuenta de administración se pueden crear reglas de supresión aplicadas a las cuentas de miembros. Para obtener más información, consulte Supresión de hallazgos de Amazon Inspector mediante reglas de supresión.

Acciones del administrador delegado

Por lo general, cuando el administrador delegado aplica la configuración a su cuenta, esa configuración se aplica a todas las demás cuentas de la organización. El administrador delegado también puede ver y recuperar la información de su propia cuenta y de cualquier miembro asociado. Desde una cuenta de administrador delegado de Amazon Inspector, se pueden realizar las siguientes acciones:

- Consultar y administrar el estado de Amazon Inspector en las cuentas asociadas, incluida la activación y desactivación de Amazon Inspector.
- Activar o desactivar los tipos de análisis para todas las cuentas de miembros de la organización.
- Consultar datos de hallazgos agregados de toda la organización y detalles de los hallazgos de todas las cuentas de miembros de la organización.
- Crear y administrar reglas de supresión que se aplican a los hallazgos en todas las cuentas de la organización.
- Activar el análisis mejorado de Amazon ECR para todos los miembros de la organización.
- Ver la cobertura de los recursos de toda la organización.
- Definir la duración de los análisis repetidos y automatizados de imágenes de contenedores de ECR para todas las cuentas de miembros de la organización. La duración del análisis que haya establecido el administrador delegado reemplaza cualquier valor que se haya establecido en una cuenta de miembro. Todas las cuentas de la organización comparten la duración de la redigitalización automática de Amazon ECR de los administradores delegados. No puede establecer diferentes duraciones de reescaneo para cuentas individuales.
- Especifique cinco rutas personalizadas para la inspección profunda de Amazon Inspector para Amazon EC2 que se utilizarán en todas las cuentas de la organización. Estas rutas se añaden a las cinco rutas personalizadas que un administrador delegado puede establecer en su cuenta. Para obtener más información sobre cómo configurar las rutas personalizadas de inspección profunda, consulteRutas personalizadas para la inspección profunda de Amazon Inspector.
- Activa y desactiva la inspección profunda de Amazon Inspector para las cuentas de los miembros.
- Exportar SBOM de las cuentas de miembros de la organización.
- Configurar el modo de análisis de Amazon EC2 para todas las cuentas de miembros de la organización. Para obtener más información, consulte Cómo administrar el modo de análisis.
- Cree y gestione las configuraciones de escaneo CIS para todas las cuentas de la organización, excepto las configuraciones de escaneo creadas por las cuentas de los miembros.

> **Note**
>
> Si la cuenta de un miembro abandona la organización, el administrador delegado ya no podrá ver las configuraciones de digitalización programadas por esa cuenta.

- Vea los resultados del escaneo CIS de todas las cuentas de la organización.

Acciones de las cuentas de miembros

La cuenta de un miembro puede ver y recuperar información sobre su cuenta en Amazon Inspector, mientras que la configuración de la cuenta la gestiona el administrador delegado. Las cuentas de miembros de una organización pueden realizar las siguientes tareas en Amazon Inspector:

- Activar Amazon Inspector en su cuenta.
- Consultar la cobertura de recursos de su cuenta.
- Ver detalles de los hallazgos de su cuenta.
- Consultar la duración de los análisis repetidos y automatizados de imágenes de contenedores de ECR para su cuenta.
- Especifique cinco rutas personalizadas para la inspección profunda de Amazon Inspector para EC2 que se utilizarán en su cuenta individual. Estas rutas se escanean además de las rutas personalizadas que el administrador delegado haya especificado para la organización. Para obtener más información sobre la configuración de las rutas de inspección profunda, consulteRutas personalizadas para la inspección profunda de Amazon Inspector.
- Vea las rutas personalizadas establecidas por el administrador delegado para la inspección exhaustiva de Amazon Inspector.
- Exportar SBOM de cualquier recurso asociado a su cuenta.
- Ver el modo de análisis de su cuenta.
- Cree y gestione las configuraciones de escaneo CIS para su cuenta.
- Vea los resultados de cualquier análisis por CIS de los recursos de su cuenta, incluidos los programados por el administrador delegado.

> **Note**
>
> Una vez que se haya activado Amazon Inspector, solo podrá desactivarlo la cuenta de administrador delegado.

Designación de un administrador delegado para Amazon Inspector

Consideraciones importantes para administradores delegados

Tome nota de los siguientes factores que definen cómo funciona el rol de administrador delegado en Amazon Inspector.

Un administrador delegado puede administrar un máximo de 5000 miembros.

Cada administrador delegado de Amazon Inspector tiene una cuota de 5000 cuentas de miembros. Sin embargo, puede haber más de 5000 cuentas en la organización. Si superas las 5000 cuentas de miembro, recibirás una notificación a través del Amazon CloudWatch Personal Health Dashboard y un correo electrónico a la cuenta del administrador delegado.

Un administrador delegado es regional.

A diferencia de AWS Organizations, Amazon Inspector es un servicio regional. Esto significa que debe designar un administrador delegado, añadir cuentas de miembros y activar los tipos de escaneo en cada uno de los sitios en los Región de AWS que desee utilizar Amazon Inspector.

Una organización solo puede tener un administrador delegado.

Solo puede haber un administrador delegado de Amazon Inspector en una organización. Si ha designado una cuenta como administrador delegado en una región, esa cuenta debe ser su administrador delegado en todas las demás regiones.

Cambiar de administrador delegado no desactivará Amazon Inspector para las cuentas de miembros.

Si eliminas al administrador delegado, Amazon Inspector no se desactivará en esas cuentas y la configuración de digitalización no se verá afectada.

Su organización de AWS debe tener activadas todas las características.

Esta es la configuración predeterminada de. AWS Organizations Si no está activada, consulte Activar todas las funciones de su organización.

Permisos necesarios para designar un administrador delegado

Debe tener permiso para activar Amazon Inspector y designar un administrador delegado de Amazon Inspector.

Agregue la siguiente instrucción al final de una política de IAM para otorgar estos permisos.

```
{
    "Sid": "PermissionsForInspectorAdmin",
    "Effect": "Allow",
    "Action": [
        "inspector2:EnableDelegatedAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
    ],
    "Resource": "*"
}
```

Designación de un administrador delegado para su organización de AWS

En el siguiente procedimiento, se muestra cómo designar un administrador delegado para una organización de AWS. Cuando se complete esta designación, Amazon Inspector se activará tanto para la cuenta de administración de Organizations como para la cuenta del administrador delegado elegida.

> **Note**
>
> Solo la cuenta de administración de Organizations puede designar un administrador delegado.

Al activar Amazon Inspector por primera vez, se crea el rol vinculado al servicio (SLR) `AWSServiceRoleForAmazonInspector` para la cuenta. Para obtener más información sobre cómo utiliza Amazon Inspector los roles vinculados a servicios, consulte Uso de roles vinculados

a servicios para Amazon Inspector. Para obtener información acerca de los roles vinculados a servicios, consulte Uso de roles vinculados a servicios en la Guía del usuario de IAM.

Designación de un administrador delegado para Amazon Inspector

Console

Designación de un administrador delegado en la consola

1. Inicie sesión en la AWS Management Console mediante la cuenta de administración de AWS Organizations.
2. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home y, a continuación, utilice el Región de AWS selector de la esquina superior derecha para especificar la región en la que desea designar un administrador.
3. En el panel Administrador delegado, introduzca el ID de cuenta de doce dígitos del Cuenta de AWS que desee designar como administrador delegado de Amazon Inspector para su organización. A continuación, elija Administración delegada.
4. (Recomendado) Repita los pasos anteriores en cada Región de AWS.

API

Designación de un administrador delegado con la API

- Ejecute la operación de la EnableDelegatedAdminAccountAPI con las credenciales de la cuenta Cuenta de AWS de administración de Organizations. También puede usar el AWS Command Line Interface para hacer esto ejecutando el siguiente comando CLI:`aws inspector2 enable-delegated-admin-account --delegated-admin-account-id 11111111111`.

> **Note**
>
> Asegúrese de especificar el ID de cuenta de la cuenta que desea convertir en administrador delegado de Amazon Inspector.

Después de especificar el administrador delegado, debe usar la cuenta de AWS Organizations administración únicamente para cambiar o eliminar la cuenta de administrador delegado.

Activación de los análisis de Amazon Inspector para cuentas de miembros

Como administrador delegado de su organización, puede activar los análisis de Amazon EC2, los análisis de Amazon ECR o ambos para cualquier miembro asociado a la cuenta de administración de AWS Organizations. Al activar los análisis para una cuenta de miembro, esa cuenta se asocia al administrador delegado, Amazon Inspector se activa automáticamente y se inician los análisis del tipo elegido al instante. Para obtener información sobre los recursos que se pueden escanear y cómo configurar los escaneos, consulte. Análisis automatizado de recursos con Amazon Inspector

Amazon Inspector ofrece varias opciones para administrar y activar los análisis de las cuentas de miembros, incluida la de permitir que las cuentas de miembros activen Amazon Inspector. Utilice una de las siguientes opciones para iniciar los análisis de las cuentas de miembros.

Activación automática de los análisis de cuentas de miembros

1. Inicie sesión en la cuenta de administrador delegado.
2. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home. A continuación, utilice el Región de AWS selector de la parte superior derecha para especificar la región en la que desea activar el escaneo de todas las cuentas de los miembros.
3. En el panel de navegación, en Configuración, elija Administración de cuentas. En la tabla de cuentas se muestran todas las cuentas de miembros asociadas a la cuenta de administración de AWS Organizations.
4. Marque la casilla de la parte superior de la tabla para seleccionar todas las cuentas de esta página. A continuación, elija Activar y elija su opción de tipo de análisis preferida en el menú.

   > **Note**
   >
   > Solo se seleccionan las cuentas actualmente visibles en la página. Si tiene varias páginas de cuentas, debe repetir este proceso en cada página. Para cambiar el número de cuentas que se muestran en la página, selecciona el icono de engranaje.

5. Active la configuración Activar automáticamente el Inspector para las cuentas de nuevos miembros y, a continuación, seleccione los tipos de escaneo para activar los nuevos miembros que se agreguen a su organización.
6. (Recomendado) Repita estos pasos en cada región en la que desee escanear las cuentas de los miembros.

El parámetro Activar Inspector automáticamente para las nuevas cuentas de miembros activa Amazon Inspector para todos los miembros futuros de la organización. Esto permite al administrador delegado de Amazon Inspector administrar cualquier miembro nuevo que se agregue a la organización. Cuando el número de cuentas de miembros alcanza la cuota de 5000, esta configuración se desactiva automáticamente. Si se elimina una cuenta y el número total de miembros disminuye por debajo de 5,000, el parámetro se reactiva automáticamente.

Activación selectiva de los análisis de cuentas de miembros

1. Inicie sesión en la cuenta de administrador delegado.
2. Abre la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home y, a continuación, utiliza el Región de AWS selector de la parte superior derecha para especificar la región en la que quieres activar el escaneo de determinadas cuentas de miembros.
3. En el panel de navegación, en Configuración, elija Administración de cuentas. En la tabla de cuentas se muestran todas las cuentas de miembros asociadas a la cuenta de administración de AWS Organizations.
4. En la página Administración de cuentas, marque la casilla para cada cuenta de miembro en la que quiera activar los análisis.
5. Seleccione Activar.
6. En el menú Activar, elija los tipos de análisis que desee activar en las cuentas seleccionadas. Puede elegir entre las siguientes opciones de análisis:
   - Todos los escaneos: para activar todos los tipos de escaneos.
   - Escaneo de EC2: para activar los escaneos de las instancias de Amazon EC2.
   - Escaneo de contenedores ECR: para activar los escaneos de imágenes de contenedores ECR.
   - AWS Lambdaescaneo estándar: para activar los escaneos de las funciones Lambda.
7. (Recomendado) Repita estos pasos en cada región en la que desee activar los escaneos para determinados miembros.

Si su cuenta AWS Organizations de administración ha delegado un administrador para Amazon Inspector, puede activar su propia cuenta como miembro y ver los detalles del escaneo de su propia cuenta.

Activación de los análisis como cuenta de miembro

1. Inicie sesión en su cuenta.
2. Abre la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home y, a continuación, utiliza el Región de AWS selector de la esquina superior derecha para especificar la región en la que quieres activar el escaneo.
3. En el panel de navegación, en Configuración, elija Administración de cuentas.
4. En la página Administración de cuentas, marque la casilla para su cuenta.
5. En el menú Activar, elija los tipos de análisis que desee activar. Puede elegir entre las siguientes opciones de análisis:
   - Todos los escaneos: para activar todos los tipos de escaneos.
   - Escaneo de EC2: para activar los escaneos de las instancias de Amazon EC2.
   - Escaneo de contenedores ECR: para activar los escaneos de imágenes de contenedores ECR.
   - AWS Lambdaescaneo estándar: para activar los escaneos de las funciones Lambda.
6. (Recomendado) Repita estos pasos en cada región en la que desee activar los escaneos.

Desasociación de cuentas de miembros en Amazon Inspector

A continuación se explica cómo desasociar cuentas de miembros. Las cuentas de miembros disociadas permanecen en su AWS Organizations organización como cuentas independientes de Amazon Inspector. El administrador delegado de Amazon Inspector ya no tiene permiso para activar y gestionar Amazon Inspector para estas cuentas. Puede volver a añadir cuentas disociadas como miembros más adelante.

> **Note**
>
> Al desasociar una cuenta, Amazon Inspector no desactiva los escaneos de esa cuenta.

Console

Para desasociar las cuentas de miembros mediante la consola

1. Inicie sesión en la cuenta del administrador delegado.

2. Abre la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home y, a continuación, utiliza el Región de AWS selector de la parte superior derecha para especificar la región en la que quieres desasociar una o más cuentas de miembros.
3. En el panel de navegación, en Configuración, elija Administración de cuentas.
4. En la página Administración de cuentas, marque la casilla para cada cuenta de miembro que quiera desasociar.
5. En el menú Acciones, selecciona Desasociar cuenta.
6. (Recomendado) Repita estos pasos en cada región en la que desee desasociar las cuentas.

API

Para desasociar las cuentas de miembros mediante la API

Use la operación de la API de DisassociateMember . En la solicitud, proporciona los ID de cuenta que vas a desasociar.

Eliminación de un administrador delegado de Amazon Inspector

Si debe asignar un nuevo administrador delegado de Amazon Inspector, puede eliminar un administrador delegado existente como cuenta de AWS Organizations gestión.

Cuando eliminas a un administrador delegado, Amazon Inspector no se desactiva en esa cuenta ni en ninguna de las cuentas de los miembros de la organización. Las cuentas de su organización se convierten en cuentas independientes y conservan la configuración de digitalización que tenían antes de ser gestionadas por un administrador delegado.

Eliminación de un administrador delegado

1. Inicie sesión en la AWS Management Console con la cuenta de administración de AWS Organizations.
2. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home y, a continuación, utilice el Región de AWS selector de la esquina superior derecha para especificar la región en la que desea eliminar al administrador delegado.
3. En el panel de navegación, en Configuración, elija Administración de cuentas.
4. En la sección Administrador delegado, elija Eliminar y confirme su acción.
5. Repita estos pasos en cada región en la que haya registrado a este administrador delegado.

Al añadir un nuevo administrador delegado de Amazon Inspector, debe asociar manualmente los miembros de la organización a la nueva cuenta de administrador. Siga los siguientes pasos para asociar a los miembros de la organización a la nueva cuenta de administrador.

Asociación de miembros con un nuevo administrador delegado

1. Inicie sesión en la AWS Management Console con la cuenta de administrador delegado.
2. Abre la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home y, a continuación, utiliza el Región de AWS selector de la parte superior derecha para especificar la región a la que quieres asociar los miembros al nuevo administrador delegado.
3. En el panel de navegación, en Configuración, elija Administración de cuentas.
4. Marque la casilla superior para seleccionar todas las cuentas enumeradas de la organización.
5. En el menú Acciones, elija Agregar miembro.
6. Repita estos pasos en cada región en la que desee asociar miembros al nuevo administrador delegado.

Supervisión del uso y los costos en Amazon Inspector

Puede utilizar la consola de Amazon Inspector y las operaciones de API para proyectar los costos mensuales por utilizar Amazon Inspector en su entorno. Si es el administrador de Amazon Inspector en un entorno con varias cuentas, puede ver el costo total de todo el entorno y las métricas de costos de cada una de las cuentas de miembros.

Utilización de la consola de uso

Puede evaluar el uso y el costo previsto de Amazon Inspector desde la consola.

Acceso a las estadísticas de uso

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. Con el selector de Región de AWS ubicado en la esquina superior derecha de la página, seleccione la región en la que desea supervisar los costos.
3. En el panel de navegación, elija Uso.

En la pestaña Por cuenta, verá el costo total previsto en función del período de 30 días indicado en Uso de la cuenta. En la tabla de la columna Costo previsto, elija un valor para ver un desglose del uso por tipo de análisis de la cuenta correspondiente. En este panel de detalles, también puede consultar los tipos de análisis que tienen una versión de prueba gratuita activa en esa cuenta.

Si es el administrador delegado de una organización, en la tabla verá una fila en la tabla para cada cuenta de la organización. Si se desasocia una cuenta de la organización, la consola mostrará su costo previsto como -.

En la pestaña Por tipo de análisis, verá un desglose del uso real hasta la fecha por tipo de análisis en el período actual de 30 días. Esta información se utiliza para calcular los costos previstos en la pestaña Por cuenta.

Si es el administrador delegado de una organización, verá el uso de cada cuenta de la organización.

En esta pestaña, puede expandir cualquier de los paneles siguientes para consultar las estadísticas de uso:

Análisis de Amazon EC2

La consola de uso de Amazon Inspector realiza un seguimiento de las siguientes métricas para el escaneo basado en agentes y el escaneo sin agente:

- Instancias (promedio): Amazon Inspector utiliza las horas de cobertura para calcular el promedio de recursos de los análisis de instancias de EC2. El resultado del promedio es el total de horas de cobertura dividido entre 720 horas (la cantidad de horas en 30 días).
- Horas de cobertura: en el caso de los análisis de Amazon EC2, indica el total de horas en los últimos 30 días que Amazon Inspector proporcionó cobertura activa para cada instancia de EC2 de una cuenta. En el caso de las instancias de EC2, las horas de cobertura son las horas transcurridas desde que Amazon Inspector descubrió la instancia hasta que finalizó, se detuvo o se excluyó de los análisis con etiquetas. Al reiniciar una instancia detenida o eliminar una etiqueta de exclusión, Amazon Inspector reanuda la cobertura y se seguirán acumulando las horas de cobertura de dicha instancia.

Escaneos de instancias CIS: el número total de escaneos CIS realizados para las instancias de la cuenta.

Análisis de Amazon ECR

Análisis iniciales: el total de primeros análisis de imágenes de la cuenta en los últimos 30 días.

Análisis repetidos: el total de análisis repetidos de imágenes de la cuenta en los últimos 30 días. Se considera como análisis repetido cualquier análisis realizado en una imagen de ECR que Amazon Inspector ya haya analizado. Si ha configurado el repositorio de ECR para que se analice continuamente, se producirán análisis repetidos automáticamente cuando Amazon Inspector añada una nueva lista de vulnerabilidades y riesgos comunes (CVE) a la base de datos.

Análisis de Lambda

La consola de uso de Amazon Inspector realiza un seguimiento de las siguientes métricas para el escaneo estándar Lambda y el escaneo de código Lambda:

- Número de funciones Lambda (promedio): Amazon Inspector utiliza las horas de cobertura para calcular el número medio de funciones para el escaneo de funciones Lambda. El resultado del promedio es el total de horas de cobertura dividido entre 720 horas (la cantidad de horas en 30 días).
- Horas de cobertura: en el caso de los análisis de funciones de Lambda, indica el total de horas en los últimos 30 días que Amazon Inspector proporcionó cobertura activa para cada función de Lambda de una cuenta. En el caso de las funciones de AWS Lambda, las horas de

cobertura se calculan desde que Amazon Inspector detecta una función hasta que se elimina o se excluye de los análisis. Si se vuelve a incluir una función excluida, se seguirán acumulando las horas de cobertura de dicha función.

Explicación de cómo Amazon Inspector calcula los costos de uso

Los costos que proporciona Amazon Inspector son estimaciones, y no costos reales, por lo que pueden diferir de los que se muestran en la consola de AWS Billing.

Tenga en cuenta la siguiente información relacionada con los cálculos de costos de Amazon Inspector en la página Uso:

- El costo de uso se aplica únicamente a la región actual. Los precios por tipo de análisis varían según la región de AWS. Para conocer los precios exactos por región, consulte la página de precios de Amazon Inspector.
- Todas las proyecciones de uso se redondean a la cantidad entera más cercana en dólares.
- Los descuentos no se incluyen en los costos previstos.
- El costo previsto representa el costo total durante un período de uso de 30 días por tipo de análisis. Si ha habido menos de 30 días de uso en una cuenta, Amazon Inspector proyecta el costo tras 30 días como si los recursos cubiertos actualmente siguieran cubiertos durante el resto del período de 30 días.
- El costo por tipo de análisis se calcula de la siguiente forma:
  - Análisis de EC2: el costo refleja el promedio de instancias de EC2 cubiertas por Amazon Inspector en los últimos 30 días.
  - Análisis de contenedores de ECR: el costo refleja la suma de análisis iniciales de imágenes y análisis repetidos de imágenes en los últimos 30 días.
  - Análisis estándar de Lambda: el costo refleja el promedio de funciones de Lambda cubiertas por Amazon Inspector en los últimos 30 días.
  - Análisis de código de Lambda: el costo refleja el promedio de funciones de Lambda cubiertas por Amazon Inspector en los últimos 30 días.

Acerca de la prueba gratuita de Amazon Inspector

Cuando activa un tipo de análisis de Amazon Inspector, se le inscribe automáticamente en una prueba gratuita de 15 días para ese tipo de análisis. Cada tipo de análisis (análisis de EC2, análisis

de ECR, análisis estándar de Lambda y análisis de código de Lambda) tiene una versión de prueba gratuita independiente.

> **Note**
>
> La versión de prueba gratuita no se aplica al escaneo CIS.

Si desactiva un tipo de análisis durante la prueba gratuita, esta se detendrá para ese tipo de análisis. Si reactiva el servicio, la prueba gratuita se reanudará y obtendrá los días restantes de la versión de prueba gratuita correspondiente.

La seguridad en Amazon Inspector

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de conformidad que se aplican a Amazon Inspector, consulte AWS Servicios dentro del alcance por programa de conformidad AWS Servicios incluidos .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayudará a comprender cómo aplicar el modelo de responsabilidad compartida cuando utilice Amazon Inspector. En los siguientes apartados, se le mostrará cómo configurar Amazon Inspector para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de Amazon Inspector.

Temas

Protección de datos en Amazon Inspector

El modelo de se aplica a protección de datos en Amazon Inspector. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog AWS Shared Responsibility Model and GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

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 Amazon Inspector u otro Servicios de AWS dispositivo mediante la consola, la API o AWS los SDK. AWS CLI Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos

encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Temas

Cifrado en reposo

Amazon Inspector almacena de forma segura los datos en reposo mediante soluciones de AWS cifrado de forma predeterminada. Amazon Inspector cifra los datos, como el inventario de recursos recopilado mediante AWS Systems Manager, el inventario de recursos analizado a partir de imágenes de Amazon ECR y los hallazgos de seguridad generados, mediante claves de cifrado AWS propias de AWS Key Management Service ().AWS KMS No puede ver, administrar ni usar las claves AWS propias, ni auditar su uso. Sin embargo, no tiene que realizar ninguna acción ni cambiar ningún programa para proteger las claves que cifran sus datos. Para obtener más información, consulte Claves propiedad de AWS.

Al deshabilitar Amazon Inspector, se eliminan permanentemente todos los recursos almacenados o mantenidos, incluidos los inventarios recopilados y los hallazgos de seguridad.

Cifrado de código en reposo en los hallazgos

Para el escaneo de código Lambda de Amazon Inspector, Amazon Inspector colabora con el objetivo de CodeGuru escanear el código en busca de vulnerabilidades. Cuando se detecta una vulnerabilidad, CodeGuru extrae un fragmento del código que contiene la vulnerabilidad y lo almacena hasta que Amazon Inspector solicite acceso. De forma predeterminada, CodeGuru utiliza una AWS clave propia para cifrar el código extraído; sin embargo, puede configurar Amazon Inspector para que utilice su propia AWS KMS clave gestionada por el cliente para el cifrado.

En el siguiente flujo de trabajo se describe cómo Amazon Inspector utiliza la clave que ha configurado para cifrar el código:

1. Usted proporciona una AWS KMS clave a Amazon Inspector mediante la UpdateEncryptionKeyAPI de Amazon Inspector.
2. Amazon Inspector reenvía la información sobre tu AWS KMS clave a CodeGuru. CodeGuru almacena la información para usarla en el futuro.

3. CodeGuru solicita una concesión AWS KMS para la clave que configuraste en Amazon Inspector.
4. CodeGuru crea una clave de datos cifrada a partir de su AWS KMS clave y la almacena. Esta clave de datos se utiliza para cifrar los datos de código almacenados por CodeGuru.
5. Siempre que Amazon Inspector solicita datos de escaneos de código, CodeGuru utiliza la autorización para descifrar la clave de datos cifrados y, a continuación, utiliza esa clave para descifrar los datos y poder recuperarlos.

Al deshabilitar el escaneo de código Lambda, CodeGuru se retira la concesión y se elimina la clave de datos asociada.

Permisos para el cifrado de código con una clave administrada por el cliente

Para usar el cifrado, debe tener una política que permita el acceso a AWS KMS las acciones, así como una declaración que otorgue a Amazon Inspector y CodeGuru permisos para usar esas acciones a través de claves de condición.

Si quiere configurar, actualizar o restablecer la clave de cifrado de su cuenta, deberá utilizar una política de administrador de Amazon Inspector como, por ejemplo, AWS política gestionada: AmazonInspector2FullAccess. También tendrá que conceder los siguientes permisos a los usuarios con permisos de solo lectura que necesiten recuperar fragmentos de código de hallazgos y datos relacionados con la clave de cifrado elegida.

En el caso de KMS, la política debe permitirle realizar las siguientes acciones:

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKeyWithoutPlainText`
- `kms:Encrypt`
- `kms:RetireGrant`

Una vez que hayas comprobado que tienes los AWS KMS permisos correctos en tu política, debes adjuntar una declaración que autorice a Amazon Inspector y CodeGuru a utilizar tu clave para el cifrado. La instrucción de política que debe adjuntar es la siguiente:

> **Note**
>
> Sustituya la región por la AWS región en la que está activado el escaneo de códigos de Amazon Inspector Lambda.

```
{
            "Sid": "allow CodeGuru Security to request a grant for a AWS KMS key",
          "Effect": "Allow",
          "Action": "kms:CreateGrant",
          "Resource": "*",
          "Condition": {
           "ForAllValues:StringEquals": {
            "kms:GrantOperations": [
             "GenerateDataKey",
             "GenerateDataKeyWithoutPlaintext",
             "Encrypt",
             "Decrypt",
             "RetireGrant",
             "DescribeKey"
            ]
           },
           "StringEquals": {
            "kms:ViaService": [
             "codeguru-security.Region.amazonaws.com"
            ]
           }
          }
         },
         {
          "Sid": "allow Amazon Inspector and CodeGuru Security to use your AWS KMS key",
          "Effect": "Allow",
          "Action": [
           "kms:Encrypt",
           "kms:Decrypt",
           "kms:RetireGrant",
           "kms:DescribeKey",
           "kms:GenerateDataKeyWithoutPlaintext"
          ],
          "Resource": "*",
          "Condition": {
```

```
          "StringEquals": {
           "kms:ViaService": [
            "inspector2.Region.amazonaws.com",
            "codeguru-security.Region.amazonaws.com"
           ]
          }
         }
        }
```

> **Note**
>
> Cuando agregue la instrucción, asegúrese de que la sintaxis sea válida. Las políticas utilizan el formato JSON. Esto significa que tiene que insertar una coma al principio o al final de la instrucción, dependiendo del lugar de la política al que agregue la instrucción. Si agrega la instrucción como la última instrucción, inserte la coma después del corchete de cierre de la instrucción anterior. Si la agrega como primera instrucción o entre dos instrucciones existentes, inserte la coma después del corchete de cierre de la instrucción que acaba de agregar.

Configuración del cifrado con una clave administrada por el cliente

Para configurar el cifrado en su cuenta con una clave administrada por el cliente, debe ser administrador de Amazon Inspector y contar con los permisos que se indican en Permisos para el cifrado de código con una clave administrada por el cliente. Además, necesitará una AWS KMS clave en la misma AWS región que sus hallazgos o una clave multirregional. Puede usar una clave simétrica existente en su cuenta o crear una clave simétrica administrada por el cliente mediante la consola de AWS administración o las API. AWS KMS Para obtener más información, consulte Creación de AWS KMS claves de cifrado simétricas en la guía del AWS KMS usuario.

Uso de la API de Amazon Inspector para configurar el cifrado

Para configurar una clave de cifrado, el UpdateEncryptionKeyfuncionamiento de la API de Amazon Inspector cuando se ha iniciado sesión como administrador de Amazon Inspector. En la solicitud de API, usa el `kmsKeyId` campo para especificar el ARN de la AWS KMS clave que deseas usar. Para `scanType`, introduzca `CODE` y, para `resourceType`, introduzca `AWS_LAMBDA_FUNCTION`.

Puedes usar la UpdateEncryptionKeyAPI para comprobar qué AWS KMS clave utiliza Amazon Inspector para el cifrado.

> **Note**
>
> Si intentas utilizarla sin `GetEncryptionKey` configurar una clave gestionada por el cliente, la operación devolverá un `ResourceNotFoundException` error, lo que significa que se está utilizando una AWS clave propia para el cifrado.

Si eliminas la clave o cambias su política de denegar el acceso a Amazon Inspector o no CodeGuru podrás acceder a los hallazgos de vulnerabilidad de tu código, el escaneo de código Lambda no funcionará en tu cuenta.

Puede utilizarla `ResetEncryptionKey` para volver a utilizar una clave AWS propia para cifrar el código extraído como parte de las conclusiones de Amazon Inspector.

Cifrado en tránsito

AWS cifra todos los datos en tránsito entre los sistemas AWS internos y otros AWS servicios.

Para la recopilación de inventario, Systems Manager recopila datos de telemetría de las instancias EC2 propiedad del cliente y los envía a AWS través de un canal protegido por Transport Layer Security (TLS) para su evaluación. Consulte Protección de datos en Systems Manager para comprender cómo SSM cifra los datos en tránsito.

Del mismo modo, los resultados de los escaneos de funciones de Amazon ECR y AWS Lambda que se envían a Security Hub se cifran mediante un canal protegido por TLS.

Identity and Access Management para Amazon Inspector

AWS Identity and Access Management (IAM) es un sistema Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los recursos. AWS Los administradores de IAM controlan a qué personas se puede autenticar (pueden iniciar sesión) y autorizar (tienen permisos) para utilizar recursos de Amazon Inspector. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades

- Administración de acceso mediante políticas
- Cómo funciona Amazon Inspector con IAM
- Ejemplos de políticas de Amazon Inspector basadas en identidades
- AWS políticas gestionadas para Amazon Inspector
- Uso de roles vinculados a servicios para Amazon Inspector
- Solución de problemas de identidad y acceso de Amazon Inspector

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realice en Amazon Inspector.

Usuario de servicio: si utiliza el servicio Amazon Inspector para trabajar, el administrador le proporcionará las credenciales y los permisos que necesite. A medida que utilice más características de Amazon Inspector para trabajar, 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 característica de Amazon Inspector, consulte Solución de problemas de identidad y acceso de Amazon Inspector.

Administrador de servicio: si está a cargo de los recursos de Amazon Inspector de su empresa, probablemente tenga acceso completo a Amazon Inspector. Su trabajo consiste en determinar a qué características y recursos de Amazon Inspector deben acceder sus usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo la empresa puede utilizar IAM con Amazon Inspector, consulte Cómo funciona Amazon Inspector con IAM.

Administrador de IAM: si es administrador de IAM, es posible que desee obtener información sobre cómo escribir políticas para gestionar el acceso a Amazon Inspector. Para consultar ejemplos de políticas basadas en la identidad de Amazon Inspector que puede utilizar en IAM, consulte Ejemplos de políticas de Amazon Inspector basadas en identidades.

Autenticación con identidades

La autenticación es la forma de iniciar sesión para AWS usar sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS 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 Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice 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 más información, consulte ¿Qué es IAM Identity Center? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede

asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos 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. El Centro de identidades de IAM correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder sus identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para

obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

- Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede agregar las políticas de IAM a los roles y los usuarios pueden asumir esos roles.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

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.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifique el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (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. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para más información sobre Organizations 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 identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar 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 Amazon Inspector con IAM

Antes de utilizar IAM para administrar el acceso a Amazon Inspector, infórmese sobre qué características de IAM se encuentran disponibles con Amazon Inspector.

Características de IAM que puede utilizar con Amazon Inspector

Característica de IAM	Soporte de Amazon Inspector
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo Amazon Inspector y otros Servicios de AWS funcionan con la mayoría de las funciones de IAM, consulte Servicios de AWS Cómo funcionan con IAM en la Guía del usuario de IAM.

Políticas de Amazon Inspector basadas en identidades

Compatibilidad con las políticas basadas en identidades	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas de Amazon Inspector basadas en identidades

Para ver ejemplos de políticas basadas en identidades de Amazon Inspector, consulte Ejemplos de políticas de Amazon Inspector basadas en identidades.

Políticas basadas en recursos de Amazon Inspector

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico.

Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Acciones de la política de Amazon Inspector

Admite acciones de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de Amazon Inspector, consulte Acciones definidas por Amazon Inspector en la Referencia de autorizaciones de servicio.

En las acciones de políticas de Amazon Inspector, se utiliza el siguiente prefijo antes de la acción:

```
inspector2
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "inspector2:action1",
      "inspector2:action2"
         ]
```

Para ver ejemplos de políticas basadas en identidades de Amazon Inspector, consulte Ejemplos de políticas de Amazon Inspector basadas en identidades.

Recursos de políticas para Amazon Inspector

Admite recursos de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `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 comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de tipos de recursos de Amazon Inspector y sus ARN, consulte Tipos de recurso definidos por Amazon Inspector en la Referencia de autorizaciones de servicio. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por Amazon Inspector.

Para ver ejemplos de políticas basadas en identidades de Amazon Inspector, consulte Ejemplos de políticas de Amazon Inspector basadas en identidades.

Claves de condición de Amazon Inspector

Admite claves de condición de políticas específicas del servicio	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen 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 lógica `AND`. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de Amazon Inspector, consulte Claves de condición de Amazon Inspector en la Referencia de autorizaciones de servicio. Para obtener más información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por Amazon Inspector.

Para ver ejemplos de políticas basadas en identidades de Amazon Inspector, consulte Ejemplos de políticas de Amazon Inspector basadas en identidades.

ACL en Amazon Inspector

Admite las 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.

ABAC con Amazon Inspector

Admite ABAC (etiquetas en las políticas)	Parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Amazon Inspector

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Permisos de entidades principales entre servicios de Amazon Inspector

Admite Forward access sessions (FAS)	Sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio de Amazon Inspector

Compatible con funciones 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 puede crear, modificar y eliminar un rol de servicio desde IAM. Para más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Amazon Inspector. Edite los roles de servicio solo cuando Amazon Inspector proporcione instrucciones para hacerlo.

Roles vinculados a servicios de Amazon Inspector

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 el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información acerca de cómo crear o administrar roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas de Amazon Inspector basadas en identidades

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar los recursos de Amazon Inspector. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que

necesitan. A continuación, el administrador puede agregar las políticas de IAM a roles, y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

A fin de obtener más información sobre las acciones y los tipos de recursos definidos por Amazon Inspector, incluido el formato de los ARN para cada tipo de recurso, consulte Acciones, recursos y claves de condición de Amazon Inspector en la Referencia de autorizaciones de servicio.

Temas

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan quién puede crear, eliminar o acceder a los recursos de Amazon Inspector de la cuenta. Estas acciones pueden generar costes adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía del usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola de Amazon Inspector

Para acceder a la consola de Amazon Inspector, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle mostrar y consultar los detalles sobre los recursos de Amazon Inspector en la cuenta de Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realizan llamadas a la API o a la AWS CLI API. AWS En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola de Amazon Inspector, adjunta también la política `ReadOnly` AWS gestionada `ConsoleAccess` o de Amazon

Inspector a las entidades. Para más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Permitir el acceso de solo lectura a todos los recursos de Amazon Inspector

En este ejemplo se muestra una política que permite el acceso de solo lectura a todos los recursos de Amazon Inspector.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "inspector2:Describe*",
                "inspector2:Get*",
                "inspector2:BatchGet*",
                "inspector2:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

Permitir el acceso completo a todos los recursos de Amazon Inspector

En este ejemplo se muestra una política que permite el acceso completo a todos los recursos de Amazon Inspector.

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

```
            "Action": "inspector2:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "inspector2.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS políticas gestionadas para Amazon Inspector

Una política AWS gestionada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen

todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AWS política gestionada: AmazonInspector2FullAccess

Puede adjuntar la política de `AmazonInspector2FullAccess` a las identidades de IAM.

Esta política concede permisos administrativos que ofrecen acceso completo a Amazon Inspector.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `inspector2`: permite el acceso completo a la funcionalidad de Amazon Inspector.
- `iam`: permite a Amazon Inspector crear el rol vinculado a servicios `AmazonInspector2AgentlessServiceRole`. Este rol es necesario para que Amazon Inspector pueda realizar operaciones como obtener información sobre las instancias de Amazon EC2 y los repositorios e imágenes de contenedores de Amazon ECR, analizar la red de VPC y describir las cuentas asociadas a la organización. Para obtener más información, consulte Uso de roles vinculados a servicios para Amazon Inspector.
- `organizations`: permite a los administradores utilizar Amazon Inspector para una organización en AWS Organizations. Tras activar el acceso de confianza para Amazon Inspector en AWS

Organizations, los miembros de la cuenta de administrador delegado pueden gestionar la configuración y ver los resultados de toda la organización.

- `codeguru-security`— Permite a los administradores utilizar Amazon Inspector para recuperar fragmentos de código de información y cambiar la configuración de cifrado del código almacenado por CodeGuru Seguridad. Para obtener más información, consulte Cifrado de código en reposo en los hallazgos .

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "inspector2:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "codeguru-security:BatchGetFindings",
    "codeguru-security:GetAccountConfiguration",
    "codeguru-security:UpdateAccountConfiguration"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "iam:CreateServiceLinkedRole",
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "iam:AWSServiceName": "inspector2.amazonaws.com"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": [
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
```

```
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS política gestionada: AmazonInspector2ReadOnlyAccess

Puede adjuntar la política de `AmazonInspector2ReadOnlyAccess` a las identidades de IAM.

Esta política concede permisos que ofrecen acceso de solo lectura a Amazon Inspector.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `inspector2`: permite el acceso de solo lectura a la funcionalidad de Amazon Inspector.
- `organizations`— Permite ver los detalles sobre la cobertura de Amazon Inspector AWS Organizations para una organización.
- `codeguru-security`— Permite recuperar fragmentos de código de CodeGuru Seguridad. También permite ver la configuración de cifrado del código almacenado en CodeGuru Security.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "inspector2:BatchGet*",
```

```
    "inspector2:List*",
    "inspector2:Describe*",
    "inspector2:Get*",
    "inspector2:Search*",
    "codeguru-security:BatchGetFindings",
    "codeguru-security:GetAccountConfiguration"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS política gestionada: AmazonInspector2ManagedCisPolicy

Puede adjuntar la política `AmazonInspector2ManagedCisPolicy` a sus entidades de IAM. Esta política debe estar asociada a un rol que conceda permisos a las instancias de Amazon EC2 para ejecutar escaneos CIS de la instancia. Puede usar una función de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y que realizan solicitudes a la API AWS CLI . AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un AWS rol a una instancia EC2 y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `inspector2`— Permite el acceso a las acciones utilizadas para ejecutar los escaneos de CIS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
            "inspector2:StartCisSession",
            "inspector2:StopCisSession",
            "inspector2:SendCisSessionTelemetry",
            "inspector2:SendCisSessionHealth"
```

```
            ],
            "Resource": "*",
        }
    ]
}
```

AWS política gestionada: AmazonInspector2ServiceRolePolicy

No puede adjuntar la política `AmazonInspector2ServiceRolePolicy` a sus entidades de IAM. Esta política está asociada a un rol vinculado a servicios que permite que Amazon Inspector realice acciones en su nombre. Para obtener más información, consulte Uso de roles vinculados a servicios para Amazon Inspector.

AWS política gestionada: AmazonInspector2AgentlessServiceRolePolicy

No puede adjuntar la política `AmazonInspector2AgentlessServiceRolePolicy` a sus entidades de IAM. Esta política está asociada a un rol vinculado a servicios que permite que Amazon Inspector realice acciones en su nombre. Para obtener más información, consulte Uso de roles vinculados a servicios para Amazon Inspector.

Amazon Inspector actualiza las políticas AWS gestionadas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de Amazon Inspector desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de Amazon Inspector.

Cambio	Descripción	Fecha
AmazonInspector2 ManagedCisPolicy — Nueva política	Amazon Inspector ha agregado una nueva política de administración que puede usar como parte de un perfil de instancia para permitir los escaneos de CIS en una instancia.	23 de enero de 2024

Cambio	Descripción	Fecha
AmazonInspector2 ServiceRolePolicy — Actualizaciones de una política existente	Amazon Inspector ha añadido nuevos permisos que permiten a Amazon Inspector iniciar escaneos CIS en las instancias de destino.	23 de enero de 2024
AmazonInspector2 AgentlessServiceRolePolicy — Nueva política	Amazon Inspector ha agregado un nuevo rol vinculado a un servicio para permitir el análisis sin agente de la instancia de EC2.	27 de noviembre de 2023
AmazonInspector2ReadOnlyAccess — Actualizaciones de una política existente	Amazon Inspector ha agregado nuevos permisos que permiten a los usuarios de solo lectura obtener detalles sobre la inteligencia de vulnerabilidades de hallazgos de vulnerabilidades de paquetes.	22 de septiembre de 2023
AmazonInspector2 ServiceRolePolicy — Actualizaciones de una política existente	Amazon Inspector ha agregado nuevos permisos que permiten a Amazon Inspector analizar las configuraciones de red de las instancias de Amazon EC2 que forman parte de los grupos de destino de Elastic Load Balancing.	31 de agosto de 2023

Cambio	Descripción	Fecha
AmazonInspector2 ReadOnlyAccess — Actualizaciones de una política existente	Amazon Inspector ha agregado nuevos permisos que permiten a los usuarios de solo lectura exportar listados de componentes de software (SBOM) de sus recursos.	29 de junio de 2023
AmazonInspector2 ReadOnlyAccess — Actualizaciones de una política existente	Amazon Inspector ha agregado nuevos permisos que permiten a los usuarios de solo lectura obtener detalles de la configuración de cifrado de los hallazgos de análisis de código de Lambda de su cuenta.	13 de junio de 2023
AmazonInspector2 FullAccess — Actualizaciones de una política existente	Amazon Inspector ha agregado nuevos permisos que permiten a los usuarios configurar un clave de KMS administrada por el cliente para cifrar el código en los hallazgos de análisis de código de Lambda.	13 de junio de 2023
AmazonInspector2 ReadOnlyAccess — Actualizaciones de una política existente	Amazon Inspector ha agregado nuevos permisos que permiten a los usuarios de solo lectura obtener detalles del estado y los hallazgos de análisis de código de Lambda de su cuenta.	2 de mayo de 2023

Cambio	Descripción	Fecha
AmazonInspector2 ServiceRolePolicy — Actualizaciones de una política existente	Amazon Inspector ha añadido nuevos permisos que permiten a Amazon Inspector crear canales AWS CloudTrail vinculados a servicios en su cuenta al activar el escaneo Lambda. Esto permite a Amazon Inspector supervisar CloudTrail los eventos de tu cuenta.	30 de abril de 2023
AmazonInspector2 FullAccess — Actualizaciones de una política existente	Amazon Inspector ha agregado nuevos permisos que permiten a los usuarios obtener detalles de los hallazgos de vulnerabilidades de código de los análisis de código de Lambda.	21 de abril de 2023
AmazonInspector2 ServiceRolePolicy — Actualizaciones de una política existente	Amazon Inspector ha añadido nuevos permisos que permiten a Amazon Inspector enviar información a Amazon EC2 Systems Manager sobre las rutas personalizadas que un cliente ha definido para la inspección profunda de Amazon EC2.	17 de abril de 2023

Cambio	Descripción	Fecha
AmazonInspector2 ServiceRolePolicy — Actualizaciones de una política existente	Amazon Inspector ha añadido nuevos permisos que permiten a Amazon Inspector crear canales AWS CloudTrail vinculados a servicios en su cuenta al activar el escaneo Lambda. Esto permite a Amazon Inspector supervisar CloudTrail los eventos de tu cuenta.	30 de abril de 2023
AmazonInspector2 ServiceRolePolicy — Actualizaciones de una política existente	Amazon Inspector ha añadido nuevos permisos que permiten a Amazon Inspector solicitar escaneos del código del desarrollador en AWS Lambda las funciones y recibir datos escaneados de Amazon CodeGuru Security. Además, Amazon Inspector ha agregado permisos para revisar las políticas de IAM. Amazon Inspector utiliza esta información para analizar las funciones de Lambda en busca de vulnerabilidades de código.	28 de febrero de 2023

Cambio	Descripción	Fecha
AmazonInspector2 ServiceRolePolicy — Actualizaciones de una política existente	Amazon Inspector ha añadido una nueva declaración que permite a Amazon Inspector recuperar información CloudWatch sobre cuándo se invocó una AWS Lambda función por última vez. Amazon Inspector utiliza esta información para centrar los análisis en las funciones de Lambda de su entorno que han estado activas durante los últimos 90 días.	20 de febrero de 2023
AmazonInspector2 ServiceRolePolicy — Actualizaciones de una política existente	Amazon Inspector ha añadido una nueva declaración que permite a Amazon Inspector recuperar información sobre AWS Lambda las funciones , incluida la versión de cada capa asociada a cada función. Amazon Inspector utiliza esta información para analizar las funciones de Lambda en busca de vulnerabilidades de seguridad.	28 de noviembre de 2022

Cambio	Descripción	Fecha
AmazonInspector2 ServiceRolePolicy — Actualizaciones de una política existente	Amazon Inspector ha agregado una nueva acción que permite a Amazon Inspector describir las ejecuciones de asociaciones de SSM. Además, Amazon Inspector ha agregado ámbitos de aplicación de recursos adicionales que permiten a Amazon Inspector crear, actualizar, eliminar e iniciar asociaciones de SSM con documentos de SSM propiedad de `AmazonInspector2` .	31 de agosto de 2022
AmazonInspector2. ServiceRolePolicy Actualizaciones de una política existente	Amazon Inspector ha actualizado el alcance de los recursos de la política para que Amazon Inspector pueda recopilar el inventario de software de otras AWS particiones.	12 de agosto de 2022
AmazonInspector2 ServiceRolePolicy — Actualizaciones de una política existente	Amazon Inspector ha reestructurado el ámbito de aplicación de recursos de las acciones para permitir que Amazon Inspector pueda crear, eliminar y actualizar asociaciones de SSM.	10 de agosto de 2022

Cambio	Descripción	Fecha
AmazonInspector2 ReadOnlyAccess — Nueva política	Amazon Inspector ha agregado una nueva política para permitir el acceso de solo lectura a la funcionalidad de Amazon Inspector.	21 de enero de 2022
AmazonInspector2 FullAccess — Nueva política	Amazon Inspector ha agregado una nueva política para permitir el acceso completo a la funcionalidad de Amazon Inspector.	29 de noviembre de 2021
AmazonInspector2 ServiceRolePolicy — Nueva política	Amazon Inspector ha agregado una nueva política que permite a Amazon Inspector realizar acciones en otros servicios en su nombre.	29 de noviembre de 2021
Amazon Inspector ha comenzado a realizar un seguimiento de los cambios	Amazon Inspector comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	29 de noviembre de 2021

Uso de roles vinculados a servicios para Amazon Inspector

Amazon Inspector utiliza un AWS Identity and Access Management rol vinculado a un servicio (IAM) denominado. `AWSServiceRoleForAmazonInspector2` El rol vinculado a servicios es un rol de IAM vinculado directamente a Amazon Inspector. Está predefinido por Amazon Inspector e incluye todos los permisos que Amazon Inspector necesita para llamar a otras Servicios de AWS personas en tu nombre.

Los roles vinculados a servicios simplifican la configuración de Amazon Inspector: ya no tendrá que agregar manualmente los permisos requeridos. Amazon Inspector define los permisos de su rol vinculado a servicios y, a menos que esté definido de otra manera, solo Amazon Inspector puede

asumir el rol. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Debe configurar permisos para permitir a una entidad de IAM (como un grupo o un rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM. Solo puede eliminar un rol vinculado a servicios después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de Amazon Inspector, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Roles vinculados a servicios. Elija una opción Sí con un enlace para revisar la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios para Amazon Inspector

Amazon Inspector usa el rol vinculado a servicios denominado `AWSServiceRoleForAmazonInspector2`. Este rol vinculado a servicios confía en el servicio `inspector2.amazonaws.com` para asumir el rol.

La política de permisos del rol, que se denomina `AmazonInspector2ServiceRolePolicy`, permite a Amazon Inspector realizar tareas como las siguientes:

- Utilizar las acciones de Amazon Elastic Compute Cloud (Amazon EC2) para obtener información acerca de las instancias y las rutas de red.
- Utilice AWS Systems Manager acciones para recuperar el inventario de sus instancias de Amazon EC2 y para recuperar información sobre paquetes de terceros a partir de rutas personalizadas.
- Utilice la AWS Systems Manager `SendCommand` acción para invocar los escaneos CIS de las instancias de destino.
- Utilizar las acciones de Amazon Elastic Container Registry para obtener información acerca de las imágenes de contenedores.
- Utilice AWS Lambda acciones para recuperar información sobre las funciones de Lambda.
- Utilice AWS Organizations acciones para describir las cuentas asociadas.
- Utilice CloudWatch acciones para recuperar información sobre la última vez que se invocaron las funciones de Lambda.
- Utilizar determinadas acciones de IAM para obtener información acerca de las políticas de IAM que podrían provocar vulnerabilidades de seguridad en el código de Lambda.

- Utilice las acciones de CodeGuru seguridad para escanear el código de las funciones de Lambda. Amazon Inspector utiliza las siguientes acciones CodeGuru de seguridad:
  - codeguru-security: CreateScan — Otorga permiso para crear un CodeGuru escaneo de seguridad.
  - codeguru-security: GetScan — Otorga permiso para recuperar los metadatos del escaneo de seguridad. CodeGuru
  - codeguru-security: ListFindings — Otorga permiso para recuperar los hallazgos generados por Security. CodeGuru
  - codeguru-security: DeleteScansByCategory — Concede permiso a CodeGuru Seguridad para eliminar los escaneos iniciados por Amazon Inspector.
  - codeguru-security: BatchGetFindings — Otorga permiso para recuperar un lote de hallazgos específicos generados por Security. CodeGuru
- Utilizar determinadas acciones de Elastic Load Balancing para realizar análisis de red de instancias de EC2 que forman parte de grupos de destino de Elastic Load Balancing.

El rol se configura con la siguiente política de permisos.

```
    {
"Version": "2012-10-17",
"Statement": [
 {
  "Sid": "TirosPolicy",
  "Effect": "Allow",
  "Action": [
   "directconnect:DescribeConnections",
   "directconnect:DescribeDirectConnectGatewayAssociations",
   "directconnect:DescribeDirectConnectGatewayAttachments",
   "directconnect:DescribeDirectConnectGateways",
   "directconnect:DescribeVirtualGateways",
   "directconnect:DescribeVirtualInterfaces",
   "ec2:DescribeAvailabilityZones",
   "ec2:DescribeCustomerGateways",
   "ec2:DescribeInstances",
   "ec2:DescribeInternetGateways",
   "ec2:DescribeManagedPrefixLists",
   "ec2:DescribeNatGateways",
   "ec2:DescribeNetworkAcls",
   "ec2:DescribeNetworkInterfaces",
```

```
    "ec2:DescribePrefixLists",
    "ec2:DescribeRegions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayConnects",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetManagedPrefixListEntries",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "ec2:SearchTransitGatewayRoutes",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetHealth",
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListFirewalls",
    "network-firewall:ListRuleGroups",
    "tiros:CreateQuery",
    "tiros:GetQueryAnswer"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "PackageVulnerabilityScanning",
```

```
    "Effect": "Allow",
    "Action": [
     "ecr:BatchGetImage",
     "ecr:BatchGetRepositoryScanningConfiguration",
     "ecr:DescribeImages",
     "ecr:DescribeRegistry",
     "ecr:DescribeRepositories",
     "ecr:GetAuthorizationToken",
     "ecr:GetDownloadUrlForLayer",
     "ecr:GetRegistryScanningConfiguration",
     "ecr:ListImages",
     "ecr:PutRegistryScanningConfiguration",
     "organizations:DescribeAccount",
     "organizations:DescribeOrganization",
     "organizations:ListAccounts",
     "ssm:DescribeAssociation",
     "ssm:DescribeAssociationExecutions",
     "ssm:DescribeInstanceInformation",
     "ssm:ListAssociations",
     "ssm:ListResourceDataSync"
    ],
    "Resource": "*"
   },
   {
    "Sid": "LambdaPackageVulnerabilityScanning",
    "Effect": "Allow",
    "Action": [
     "lambda:ListFunctions",
     "lambda:GetFunction",
     "lambda:GetLayerVersion",
     "cloudwatch:GetMetricData"
    ],
    "Resource": "*"
   },
   {
    "Sid": "GatherInventory",
    "Effect": "Allow",
    "Action": [
     "ssm:CreateAssociation",
     "ssm:StartAssociationsOnce",
     "ssm:DeleteAssociation",
     "ssm:UpdateAssociation"
    ],
    "Resource": [
```

```
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ssm:*:*:document/AmazonInspector2-*",
    "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
    "arn:aws:ssm:*:*:managed-instance/*",
    "arn:aws:ssm:*:*:association/*"
   ]
  },
  {
   "Sid": "DataSyncCleanup",
   "Effect": "Allow",
   "Action": [
    "ssm:CreateResourceDataSync",
    "ssm:DeleteResourceDataSync"
   ],
   "Resource": [
    "arn:aws:ssm:*:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
   ]
  },
  {
   "Sid": "ManagedRules",
   "Effect": "Allow",
   "Action": [
    "events:PutRule",
    "events:DeleteRule",
    "events:DescribeRule",
    "events:ListTargetsByRule",
    "events:PutTargets",
    "events:RemoveTargets"
   ],
   "Resource": [
    "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
   ]
  },
  {
   "Sid": "LambdaCodeVulnerabilityScanning",
   "Effect": "Allow",
   "Action": [
    "codeguru-security:CreateScan",
    "codeguru-security:GetAccountConfiguration",
    "codeguru-security:GetFindings",
    "codeguru-security:GetScan",
    "codeguru-security:ListFindings",
    "codeguru-security:BatchGetFindings",
    "codeguru-security:DeleteScansByCategory"
```

```
    ],
    "Resource": [
     "*"
    ]
   },
   {
    "Sid": "CodeGuruCodeVulnerabilityScanning",
    "Effect": "Allow",
    "Action": [
     "iam:GetRole",
     "iam:GetRolePolicy",
     "iam:GetPolicy",
     "iam:GetPolicyVersion",
     "iam:ListAttachedRolePolicies",
     "iam:ListPolicies",
     "iam:ListPolicyVersions",
     "iam:ListRolePolicies",
     "lambda:ListVersionsByFunction"
    ],
    "Resource": [
     "*"
    ],
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
       "codeguru-security.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "Ec2DeepInspection",
    "Effect": "Allow",
    "Action": [
     "ssm:PutParameter",
     "ssm:GetParameters",
     "ssm:DeleteParameter"
    ],
    "Resource": [
     "arn:aws:ssm:*:*:parameter/inspector-aws/service/inspector-linux-application-paths"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
```

```
    }
   }
  },
  {
   "Sid": "AllowManagementOfServiceLinkedChannel",
   "Effect": "Allow",
   "Action": [
    "cloudtrail:CreateServiceLinkedChannel",
    "cloudtrail:DeleteServiceLinkedChannel"
   ],
   "Resource": [
    "arn:aws:cloudtrail:*:*:channel/aws-service-channel/inspector2/*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "AllowListServiceLinkedChannels",
   "Effect": "Allow",
   "Action": [
    "cloudtrail:ListServiceLinkedChannels"
   ],
   "Resource": [
    "*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "AllowToRunInvokeCisSpecificDocuments",
   "Effect": "Allow",
   "Action": [
    "ssm:SendCommand",
    "ssm:GetCommandInvocation"
   ],
   "Resource": [
    "arn:aws:ssm:*:*:document/AmazonInspector2-InvokeInspectorSsmPluginCIS"
   ]
```

```
  },
  {
   "Sid": "AllowToRunCisCommandsToSpecificResources",
   "Effect": "Allow",
   "Action": [
    "ssm:SendCommand"
   ],
   "Resource": [
    "arn:aws:ec2:*:*:instance/*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "AllowToPutCloudwatchMetricData",
   "Effect": "Allow",
   "Action": [
    "cloudwatch:PutMetricData"
   ],
   "Resource": [
    "*"
   ],
   "Condition": {
    "StringEquals": {
     "cloudwatch:namespace": "AWS/Inspector2"
    }
   }
  }
 ]
}
```

Creación de roles vinculados a servicios de Amazon Inspector

No necesita crear manualmente un rol vinculado a servicios. Al activar Amazon Inspector en la AWS Management Console AWS CLI, la o la AWS API, Amazon Inspector crea automáticamente la función vinculada al servicio.

Edición de roles vinculados a servicios de Amazon Inspector

Amazon Inspector no permite editar el rol vinculado a servicios `AWSServiceRoleForAmazonInspector2`. Después de crear un rol vinculado a servicios, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia al mismo. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Edición de un rol vinculado a un servicio en la Guía del usuario de IAM.

Eliminación de roles vinculados a servicios de Amazon Inspector

Si ya no utiliza Amazon Inspector, le recomendamos que elimine el rol vinculado a servicios `AWSServiceRoleForAmazonInspector2`. Antes de poder eliminar el rol, debes desactivar Amazon Inspector en todos los Región de AWS lugares donde esté activado. Al desactivar Amazon Inspector, no se elimina el rol. Por lo tanto, si activa Amazon Inspector de nuevo, puede utilizar el rol. De esta forma, puede evitar tener una entidad sin utilizar que no se supervise ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

Si elimina este rol vinculado a un servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al activar Amazon Inspector, Amazon Inspector vuelve a crear el rol vinculado a servicios en su nombre.

> **Note**
>
> Se podría producir un error si el servicio de Amazon Inspector está utilizando el rol cuando intente eliminar los recursos. En ese caso, espere unos minutos e intente de nuevo la operación.

Puede utilizar la consola de IAM AWS CLI, la o la AWS API para eliminar el rol vinculado al `AWSServiceRoleForAmazonInspector2` servicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Permisos de roles vinculados a servicios para análisis sin agente de Amazon Inspector

El análisis sin agente de Amazon Inspector usa el rol vinculado a servicios denominado `AWSServiceRoleForAmazonInspector2Agentless`. Este SLR permite a Amazon Inspector crear una instantánea del volumen de Amazon EBS en su cuenta y, a continuación,

acceder a los datos de dicha instantánea. Este rol vinculado a servicios confía en el servicio `agentless.inspector2.amazonaws.com` para asumir el rol.

> **Important**
>
> Las instrucciones de este rol vinculado a un servicio impiden que Amazon Inspector realice análisis sin agente en cualquier instancia de EC2 que el usuario haya excluido de las exploraciones mediante la etiqueta `InspectorEc2Exclusion`. Además, las instrucciones impiden que Amazon Inspector acceda a los datos cifrados de un volumen cuando la clave de KMS utilizada para cifrarlos tiene la etiqueta `InspectorEc2Exclusion`. Para obtener más información, consulte Exclusión de instancias de los análisis de Amazon Inspector.

La política de permisos del rol, que se denomina `AmazonInspector2AgentlessServiceRolePolicy`, permite a Amazon Inspector realizar tareas como las siguientes:

- Utilizar las acciones de Amazon Elastic Compute Cloud (Amazon EC2) para recuperar información sobre las instancias, los volúmenes y las instantáneas de EC2.
  - Utilizar las acciones de etiquetado de Amazon EC2 para etiquetar las instantáneas para los análisis con la clave de la etiqueta `InspectorScan`.
  - Utilizar las acciones de instantáneas de Amazon EC2 para crear instantáneas, etiquetarlas con la clave de la etiqueta `InspectorScan` y, a continuación, eliminar las instantáneas de los volúmenes de Amazon EBS que se hayan etiquetado con la clave de la etiqueta `InspectorScan`.
- Utilizar las acciones de Amazon EBS para recuperar información de las instantáneas etiquetadas con la clave de la etiqueta `InspectorScan`.
- Utilice determinadas acciones de AWS KMS descifrado para descifrar las instantáneas cifradas con claves gestionadas por el cliente. AWS KMS Amazon Inspector no descifra las instantáneas cuando la clave de KMS utilizada para cifrarlas está etiquetada con la etiqueta `InspectorEc2Exclusion`.

El rol se configura con la siguiente política de permisos.

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

```
"Statement": [
 {
  "Sid": "InstanceIdentification",
  "Effect": "Allow",
  "Action": [
   "ec2:DescribeInstances",
   "ec2:DescribeVolumes",
   "ec2:DescribeSnapshots"
  ],
  "Resource": "*"
 },
 {
  "Sid": "GetSnapshotData",
  "Effect": "Allow",
  "Action": [
   "ebs:ListSnapshotBlocks",
   "ebs:GetSnapshotBlock"
  ],
  "Resource": "arn:aws:ec2:*:*:snapshot/*",
  "Condition": {
   "StringLike": {
    "aws:ResourceTag/InspectorScan": "*"
   }
  }
 },
 {
  "Sid": "CreateSnapshotsAnyInstanceOrVolume",
  "Effect": "Allow",
  "Action": "ec2:CreateSnapshots",
  "Resource": [
   "arn:aws:ec2:*:*:instance/*",
   "arn:aws:ec2:*:*:volume/*"
  ]
 },
 {
  "Sid": "DenyCreateSnapshotsOnExcludedInstances",
  "Effect": "Deny",
  "Action": "ec2:CreateSnapshots",
  "Resource": "arn:aws:ec2:*:*:instance/*",
  "Condition": {
   "StringEquals": {
    "ec2:ResourceTag/InspectorEc2Exclusion": "true"
   }
  }
```

```
  },
  {
   "Sid": "CreateSnapshotsOnAnySnapshotOnlyWithTag",
   "Effect": "Allow",
   "Action": "ec2:CreateSnapshots",
   "Resource": "arn:aws:ec2:*:*:snapshot/*",
   "Condition": {
    "Null": {
     "aws:TagKeys": "false"
    },
    "ForAllValues:StringEquals": {
     "aws:TagKeys": "InspectorScan"
    }
   }
  },
  {
   "Sid": "CreateOnlyInspectorScanTagOnlyUsingCreateSnapshots",
   "Effect": "Allow",
   "Action": "ec2:CreateTags",
   "Resource": "arn:aws:ec2:*:*:snapshot/*",
   "Condition": {
    "StringLike": {
     "ec2:CreateAction": "CreateSnapshots"
    },
    "Null": {
     "aws:TagKeys": "false"
    },
    "ForAllValues:StringEquals": {
     "aws:TagKeys": "InspectorScan"
    }
   }
  },
  {
   "Sid": "DeleteOnlySnapshotsTaggedForScanning",
   "Effect": "Allow",
   "Action": "ec2:DeleteSnapshot",
   "Resource": "arn:aws:ec2:*:*:snapshot/*",
   "Condition": {
    "StringLike": {
     "ec2:ResourceTag/InspectorScan": "*"
    }
   }
  },
  {
```

```
    "Sid": "DenyKmsDecryptForExcludedKeys",
    "Effect": "Deny",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/InspectorEc2Exclusion": "true"
     }
    }
   },
   {
    "Sid": "DecryptSnapshotBlocksVolContext",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com",
      "kms:EncryptionContext:aws:ebs:id": "vol-*"
     }
    }
   },
   {
    "Sid": "DecryptSnapshotBlocksSnapContext",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com",
      "kms:EncryptionContext:aws:ebs:id": "snap-*"
     }
    }
   },
   {
    "Sid": "DescribeKeysForEbsOperations",
    "Effect": "Allow",
    "Action": "kms:DescribeKey",
```

```
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com"
     }
    }
   },
   {
    "Sid": "ListKeyResourceTags",
    "Effect": "Allow",
    "Action": "kms:ListResourceTags",
    "Resource": "arn:aws:kms:*:*:key/*"
   }
  ]
}
```

Creación de un rol vinculado a un servicio para un análisis sin agente

No necesita crear manualmente un rol vinculado a servicios. Al activar Amazon Inspector en la AWS Management Console AWS CLI, la o la AWS API, Amazon Inspector crea automáticamente la función vinculada al servicio.

Edición de un rol vinculado a un servicio para un análisis sin agente

Amazon Inspector no permite editar el rol vinculado a servicios `AWSServiceRoleForAmazonInspector2Agentless`. Después de crear un rol vinculado a servicios, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia al mismo. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Edición de un rol vinculado a un servicio en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio para un análisis sin agente

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no conservará una entidad no utilizada que no se monitoree ni se mantenga de forma activa.

> **Important**
>
> Para eliminar el rol `AWSServiceRoleForAmazonInspector2Agentless`, debe configurar el modo de análisis como basado en agentes en todas las regiones en las que esté disponible el análisis sin agente. Para obtener más información, consulte [por determinar: vínculo sobre cómo establecer el modo de análisis].

Cómo eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForAmazonInspector2Agentless servicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Solución de problemas de identidad y acceso de Amazon Inspector

Utilice la siguiente información para diagnosticar y solucionar los problemas habituales que pueden surgir cuando se trabaja con Amazon Inspector e IAM.

Temas

- No tengo autorización para llevar a cabo una acción en Amazon Inspector
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Amazon Inspector

No tengo autorización para llevar a cabo una acción en Amazon Inspector

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `inspector2:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 inspector2:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `inspector2:GetWidget`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para llevar a cabo la acción `iam:PassRole`, las políticas se deben actualizar para permitirle pasar un rol a Amazon Inspector.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado "`marymajor`" intenta utilizar la consola para realizar una acción en Amazon Inspector. Sin embargo, la acción requiere que el servicio cuente con permisos que concede un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Amazon Inspector

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si Amazon Inspector admite estas características, consulte Cómo funciona Amazon Inspector con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante la federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Supervisión de Amazon Inspector

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon Inspector y sus demás AWS soluciones. AWS proporciona herramientas de supervisión para vigilar Amazon Inspector, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- Amazon EventBridge es un servicio de bus de eventos sin servidor que facilita la conexión de sus aplicaciones con datos de diversas fuentes. EventBridge ofrece un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones de oftware-as-a S-Service (SaaS) AWS y servicios, y dirige esos datos a destinos como Lambda. Esto le permite supervisar los eventos que ocurren en los servicios y compilar arquitecturas basadas en eventos. Para obtener más información, consulta la Guía del EventBridge usuario de Amazon.
- AWS CloudTrail captura las llamadas a la API y los eventos relacionados realizados por su cuenta de Cuenta de AWS o en su nombre. CloudTrail a continuación, entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para más información, consulte la Guía del usuario de AWS CloudTrail.

Registro de llamadas a la API de Amazon Inspector con AWS CloudTrail

Amazon Inspector está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario o rol de IAM, o por un Servicio de AWS miembro de Amazon Inspector. CloudTrail captura todas las llamadas a la API de Amazon Inspector como eventos. Entre las llamadas capturadas, se incluyen las llamadas desde la consola de Amazon Inspector y las llamadas a las operaciones de la API de Amazon Inspector. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Amazon Inspector. Si no configura un registro de seguimiento, puede ver los eventos más recientes en la consola de CloudTrail en el Event history (Historial de eventos). Con la información recopilada por CloudTrail, puede determinar:

- La solicitud que se realizó a Amazon Inspector
- La dirección IP desde la que se realizó la solicitud
- Quién ha realizado la solicitud
- La hora a la que se realizó la solicitud

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Información de Amazon Inspector en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en Amazon Inspector, esa actividad se registra en un CloudTrail evento junto con otros Servicio de AWS eventos del historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los de Amazon Inspector, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. Además, puede configurar otros Servicios de AWS para que analicen más a fondo los datos de eventos recopilados en los CloudTrail registros y actúen en función de ellos. Para obtener más información, consulte los temas siguientes:

- Introducción a la creación de registros de seguimiento

- CloudTrail servicios e integraciones compatibles
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias cuentas
- Recibir archivos de CloudTrail registro de varias regiones

Todas las acciones de Amazon Inspector las registra CloudTrail. Todas las acciones que lleva a cabo Amazon Inspector se documentan en la Referencia de la API de Amazon Inspector. Por ejemplo, las llamadas a las acciones `CreateFindingsReport`, `ListCoverage`, y`UpdateOrganizationConfiguration` generan entradas en los archivos de registro de CloudTrail .

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 las credenciales del usuario raíz o del usuario de IAM.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Descripción de las entradas de archivos de registro de Amazon Inspector

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 única solicitud desde cualquier origen. Los eventos incluyen información sobre la acción solicitada, la fecha y hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un seguimiento ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

Amazon Inspector Escanea la información en CloudTrail

Amazon Inspector Scan está integrado con CloudTrail. Todas las operaciones de la API de Amazon Inspector Scan se registran como eventos de administración. Para obtener una lista de las operaciones de la API de Amazon Inspector Scan en las que Amazon Inspector inicia sesión CloudTrail, consulte Amazon Inspector Scan en la referencia de la API de Amazon Inspector.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `ScanSbom` acción:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:akua_mansa",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/akua_mansa",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-10-17T15:22:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-10-17T16:02:34Z",
    "eventSource": "gamma-inspector-scan.amazonaws.com",
    "eventName": "ScanSbom",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.0",
    "userAgent": "aws-sdk-java/2.20.162 Mac_OS_X/13.5.2 OpenJDK_64-
Bit_Server_VM/17.0.8+7-LTS Java/17.0.8 vendor/Amazon.com_Inc. io/sync http/
UrlConnection cfg/retry-mode/legacy",
    "requestParameters": {
        "sbom": {
            "specVersion": "1.5",
            "metadata": {
                "component": {
                    "name": "debian",
                    "type": "operating-system",
                    "version": "9"
                }
            },
            "components": [
```

```
                {
                    "name": "packageOne",
                    "purl": "pkg:deb/debian/packageOne@1.0.0?arch=x86_64&distro=9",
                    "type": "application"
                }
            ],
            "bomFormat": "CycloneDX"
        }
    },
    "responseElements": null,
    "requestID": "f041a27f-f33e-4f70-b09b-5fbc5927282a",
    "eventID": "abc8d1e4-d214-4f07-bc56-8a31be6e36fe",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Validación de conformidad para Amazon Inspector

Para saber si un programa de cumplimiento Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

> **Note**
>
> No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan 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 los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en Amazon Inspector

La infraestructura AWS global se basa en distintas zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. 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.

Seguridad de infraestructuras en Amazon Inspector

Como servicio gestionado, Amazon Inspector está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a Amazon Inspector a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Respuesta a incidentes en Amazon Inspector

La seguridad de AWS es nuestra mayor prioridad. Como parte del modelo de responsabilidad compartida AWS en la nube, AWS administra un centro de datos, una red y una arquitectura de software que cumplen con los requisitos de las organizaciones más sensibles a la seguridad. AWS es responsable de cualquier respuesta a un incidente relacionado con el propio AWS Config servicio. Además, como AWS cliente, usted comparte la responsabilidad de mantener la seguridad en la nube. Esto significa que usted controla la seguridad que decide implementar desde las AWS herramientas y funciones a las que tiene acceso, y es responsable de la respuesta a los incidentes, según su parte del modelo de responsabilidad compartida.

Al establecer una base de seguridad que cumpla con los objetivos de las aplicaciones que se ejecutan en la nube, puede detectar las desviaciones a las que puede responder. Dado que la respuesta a los incidentes de seguridad puede ser un tema complejo, le recomendamos que consulte los siguientes recursos para que pueda comprender mejor el impacto que la respuesta a incidentes (IR) y sus elecciones tienen en sus objetivos corporativos: la Guía de respuesta a incidentes de AWS

seguridad, el documento técnico sobre las mejores prácticas de AWS seguridad y el documento técnico sobre la perspectiva de seguridad del marco de adopción de la AWS nube (CAF).

Integraciones de Amazon Inspector

Amazon Inspector se integra con otros servicios de AWS. Estos servicios pueden ingerir datos de Amazon Inspector para que pueda ver los hallazgos de manera diferente. Consulte las siguientes opciones de integración para obtener más información acerca del funcionamiento de cada servicio con Amazon Inspector.

Integración de Amazon Inspector con Amazon ECR

Amazon Elastic Container Registry (Amazon ECR) es un registro de contenedores de Docker completamente administrado que facilita el almacenamiento, el uso compartido y la implementación de imágenes de contenedores. Los registros privados de Amazon ECR alojan las imágenes de contenedores en una arquitectura escalable y de alta disponibilidad. Puede utilizar Amazon Inspector para analizar las imágenes de contenedores que se encuentran en los repositorios de Amazon ECR en busca de paquetes de sistemas operativos y de lenguajes de programación vulnerables.

Para obtener más información acerca del uso de Amazon ECR con Amazon Inspector, consulte Integración de Amazon Inspector con Amazon Elastic Container Registry (Amazon ECR).

Integración de Amazon Inspector con AWS Security Hub

AWS Security Hub recopila datos de seguridad de todas sus cuentas y servicios de AWS, así como de otros productos compatibles, para evaluar el estado de seguridad del entorno de acuerdo con los estándares del sector y de las prácticas recomendadas. Además de evaluar el estado de seguridad, Security Hub crea una ubicación central para los hallazgos en todos los servicios de AWS integrados y productos de la red socios de AWS. Al activar Security Hub con Amazon Inspector, Security Hub incorpora automáticamente los datos de los hallazgos de Amazon Inspector.

Para obtener más información acerca del uso de Security Hub con Amazon Inspector, consulte Integración de Amazon Inspector con AWS Security Hub.

Integración de Amazon Inspector con Amazon Elastic Container Registry (Amazon ECR)

Amazon ECR es un registro de contenedores completamente administrado que admite imágenes de Docker y OCI y artefactos en AWS. Si utiliza Amazon ECR, puede activar el análisis mejorado del

registro para que Amazon Inspector detecte automáticamente las imágenes de contenedores y las escanee en busca de paquetes de sistemas operativos y de lenguajes de programación vulnerables.

Esta integración le permite ver los hallazgos de Amazon Inspector relacionados con imágenes de contenedores en la consola de Amazon ECR. Además, desde la consola de Amazon ECR, puede crear filtros de inclusión para administrar la frecuencia de análisis y limitar el alcance de los análisis.

Activación de la integración

Para activar la integración, active los análisis de Amazon Inspector a través de la consola o la API de Amazon Inspector o configure el repositorio para que utilice el análisis mejorado con Amazon Inspector a través de la consola o la API de Amazon ECR.

Para obtener más información sobre cómo activar la integración a través de Amazon Inspector, consulteAnálisis automatizado de recursos con Amazon Inspector.

Para obtener información sobre cómo activar y configurar el análisis mejorado en Amazon ECR, consulte la sección Análisis mejorado de la guía del usuario de Amazon ECR.

Uso de la integración con un entorno de varias cuentas

Si es miembro de un entorno de varias cuentas, puede activar el análisis mejorado a través de Amazon ECR. No obstante, una vez se haya activado, solo podrá desactivarlo el administrador delegado de Amazon Inspector. Si se desactiva, se volverá a utilizar el análisis básico. Para obtener más información, consulte Desactivación de Amazon Inspector.

Integración de Amazon Inspector con AWS Security Hub

Security Hub le proporciona una visión completa de su estado de seguridad en AWS y lo ayuda a verificar su entorno con los estándares y las prácticas recomendadas del sector de la seguridad. Security Hub recopila datos de seguridad de todas las cuentas y servicios de AWS, así como de otros productos compatibles. Puede utilizar la información que le proporciona para analizar las tendencias de seguridad e identificar los problemas de seguridad de mayor prioridad.

La integración de Amazon Inspector con Security Hub permite enviar hallazgos de Amazon Inspector a Security Hub. Security Hub puede incluir esos resultados en su análisis de la posición de seguridad.

En AWS Security Hub, los problemas de seguridad se rastrean como hallazgos. Algunos resultados provienen de problemas detectados por otros servicios de AWS o productos de terceros. Security

Hub también cuenta con un conjunto de reglas que utiliza para detectar problemas de seguridad y generar resultados. Security Hub proporciona herramientas para administrar los resultados de todas estas fuentes. Puede ver y filtrar listas de hallazgos y ver los detalles de un hallazgo. Para obtener más información acerca de los hallazgos en Security Hub, consulte Visualización de hallazgos en la Guía del usuario de AWS Security Hub. También puede realizar un seguimiento del estado de una investigación de un hallazgo. Consulte Adopción de medidas sobre los hallazgos en la Guía del usuario de AWS Security Hub.

Todos los resultados en Security Hub usan un formato JSON estándar denominado AWS Security Finding Format (ASFF). El ASFF incluye detalles sobre el origen del problema, los recursos afectados y el estado actual del hallazgo. Consulte Formato de hallazgo de seguridad de AWS (ASFF) en la Guía del usuario de AWS Security Hub.

Security Hub archivará los hallazgos de Amazon Inspector una vez que se hayan corregido y cerrado en Amazon Inspector.

Visualización de los hallazgos de Amazon Inspector en AWS Security Hub

Los hallazgos de Amazon Inspector Classic y de la nueva versión de Amazon Inspector están disponibles en el mismo panel de Security Hub. Ahora bien, si desea filtrar los hallazgos de la nueva versión de Amazon Inspector, añada `"aws/inspector/ProductVersion": "2"` a la barra de filtros. Al añadir este filtro, se excluyen los hallazgos de Amazon Inspector Classic del panel de Security Hub.

Ejemplo de hallazgo de Amazon Inspector


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:inspector2:us-east-1:123456789012:finding/FINDING_ID",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
  "ProductName": "Inspector",
  "CompanyName": "Amazon",
  "Region": "us-east-1",
  "GeneratorId": "AWSInspector",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
  ],
  "FirstObservedAt": "2023-01-31T20:25:38Z",
  "LastObservedAt": "2023-05-04T18:18:43Z",
  "CreatedAt": "2023-01-31T20:25:38Z",
```

```
  "UpdatedAt": "2023-05-04T18:18:43Z",
  "Severity": {
    "Label": "HIGH",
    "Normalized": 70
  },
  "Title": "CVE-2022-34918 - kernel",
  "Description": "An issue was discovered in the Linux kernel through 5.18.9. A type
 confusion bug in nft_set_elem_init (leading to a buffer overflow) could be used by a
 local attacker to escalate privileges, a different vulnerability than CVE-2022-32250.
 (The attacker can obtain root access, but must start with an unprivileged user
 namespace to obtain CAP_NET_ADMIN access.) This can be fixed in nft_setelem_parse_data
 in net/netfilter/nf_tables_api.c.",
  "Remediation": {
    "Recommendation": {
      "Text": "Remediation is available. Please refer to the Fixed version in the
 vulnerability details section above. For detailed remediation guidance for each of the
 affected packages, refer to the vulnerabilities section of the detailed finding JSON."
    }
  },
  "ProductFields": {
    "aws/inspector/FindingStatus": "ACTIVE",
    "aws/inspector/inspectorScore": "7.8",
    "aws/inspector/resources/1/resourceDetails/awsEc2InstanceDetails/platform":
 "AMAZON_LINUX_2",
    "aws/inspector/ProductVersion": "2",
    "aws/inspector/instanceId": "i-0f1ed287081bdf0fb",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
arn:aws:inspector2:us-east-1:123456789012:finding/FINDING_ID",
    "aws/securityhub/ProductName": "Inspector",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:123456789012:i-0f1ed287081bdf0fb",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Patch Group": "SSM",
        "Name": "High-SEv-Test"
      },
      "Details": {
        "AwsEc2Instance": {
          "Type": "t2.micro",
```

```
          "ImageId": "ami-0cff7528ff583bf9a",
          "IpV4Addresses": [
            "52.87.229.97",
            "172.31.57.162"
          ],
          "KeyName": "ACloudGuru",
          "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/
AmazonSSMRoleForInstancesQuickSetup",
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-9c934cb1",
          "LaunchedAt": "2022-07-26T21:49:46Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "Vulnerabilities": [
    {
      "Id": "CVE-2022-34918",
      "VulnerablePackages": [
        {
          "Name": "kernel",
          "Version": "5.10.118",
          "Epoch": "0",
          "Release": "111.515.amzn2",
          "Architecture": "X86_64",
          "PackageManager": "OS",
          "FixedInVersion": "0:5.10.130-118.517.amzn2",
          "Remediation": "yum update kernel"
        }
      ],
      "Cvss": [
        {
          "Version": "2.0",
          "BaseScore": 7.2,
          "BaseVector": "AV:L/AC:L/Au:N/C:C/I:C/A:C",
          "Source": "NVD"
        },
        {
          "Version": "3.1",
```

```
          "BaseScore": 7.8,
          "BaseVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
          "Source": "NVD"
        },
        {
          "Version": "3.1",
          "BaseScore": 7.8,
          "BaseVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
          "Source": "NVD",
          "Adjustments": []
        }
      ],
      "Vendor": {
        "Name": "NVD",
        "Url": "https://nvd.nist.gov/vuln/detail/CVE-2022-34918",
        "VendorSeverity": "HIGH",
        "VendorCreatedAt": "2022-07-04T21:15:00Z",
        "VendorUpdatedAt": "2022-10-26T17:05:00Z"
      },
      "ReferenceUrls": [
        "https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?
id=7e6bc1f6cabcd30aba0b11219d8e01b952eacbb6",
        "https://lore.kernel.org/netfilter-devel/cd9428b6-7ffb-dd22-d949-
d86f4869f452@randorisec.fr/T/",
        "https://www.debian.org/security/2022/dsa-5191"
      ],
      "FixAvailable": "YES"
    }
  ],
  "FindingProviderFields": {
    "Severity": {
      "Label": "HIGH"
    },
    "Types": [
      "Software and Configuration Checks/Vulnerabilities/CVE"
    ]
  },
  "ProcessedAt": "2023-05-05T20:28:38.822Z"
}
```

Activación y configuración de la integración

Para utilizar la integración de Amazon Inspector con AWS Security Hub, es necesario activar Security Hub. Para obtener información sobre cómo activar Security Hub, consulte Configuración de Security Hub en la Guía del usuario de AWS Security Hub.

Una vez Amazon Inspector y Security Hub estén activados, la integración se activa automáticamente y Amazon Inspector comienza a enviar los hallazgos a Security Hub. Amazon Inspector envía todos los hallazgos que genera a Security Hub en formato AWS Security Finding Format (ASFF).

Interrupción de la publicación de hallazgos en AWS Security Hub

Cómo dejar de enviar hallazgos

Para dejar de enviar resultados a Security Hub, puede utilizar la consola de Security Hub o la API.

Consulte Desactivación y activación del flujo de hallazgos desde una integración (consola) o Desactivación del flujo de hallazgos desde una integración (API de Security Hub, AWS CLI) en la Guía del usuario de AWS Security Hub.

Sistemas operativos y lenguajes de programación admitidos en Amazon Inspector

Amazon Inspector puede escanear aplicaciones de software instaladas en instancias de Amazon Elastic Compute Cloud (Amazon EC2), imágenes de contenedores almacenadas en los repositorios de Amazon Elastic Container Registry (Amazon ECR) y funciones. AWS Lambda En el caso de las imágenes de contenedores ECR, Amazon Inspector puede buscar vulnerabilidades en los paquetes del sistema operativo y del lenguaje de programación. En el caso de las funciones Lambda, Amazon Inspector puede buscar vulnerabilidades en el código. Cuando Amazon Inspector analiza recursos, utiliza su propio motor de análisis, creado específicamente para ello, para obtener más de 50 fuentes de datos con las que generar hallazgos asociados a vulnerabilidades y riesgos comunes (CVE). Las fuentes pueden ser avisos de seguridad de proveedores, NVD, MITRE, fuentes de código abierto, investigaciones internas y fuentes de datos con licencia.

Para que Amazon Inspector analice un recurso, el recurso debe ejecutar un sistema operativo compatible o utilizar un lenguaje de programación admitido. En los temas de esta sección se enumeran los sistemas operativos, los tiempos de ejecución y los lenguajes de programación que Amazon Inspector admite actualmente para distintos recursos y tipos de escaneo. También enumeran los sistemas operativos que Amazon Inspector admitía anteriormente, pero que desde entonces los proveedores han dejado de usar. Amazon Inspector solo puede ofrecer compatibilidad limitada con un sistema operativo una vez que el proveedor suspende la compatibilidad con este.

Temas

Sistemas operativos admitidos: análisis de Amazon EC2

En la siguiente tabla se enumeran los sistemas operativos que Amazon Inspector admite actualmente para los escaneos de instancias de Amazon EC2. También se indica el origen de las advertencias de seguridad del proveedor para cada una de ellas y si ese sistema operativo se puede escanear mediante el método de escaneo con o sin agente. Para obtener más información sobre los métodos de análisis, consulte Análisis basado en agentes y Análisis sin agente.

> **Note**
>
> Las detecciones del sistema operativo Linux solo se admiten en el repositorio predeterminado del administrador de paquetes y no incluyen aplicaciones de terceros, repositorios de soporte ampliado (por ejemplo, BYOS RHEL, PAYG RHEL y RHEL para SAP) ni repositorios opcionales, como Red Hat Application Streams.

Sistema operativo	Versión	Avisos de seguridad del proveedor	Compatibilidad con el análisis sin agente	Compatibilidad con el análisis basado en agentes
AlmaLinux	8	ALSA	Sí	Sí
AlmaLinux	9	ALSA	Sí	Sí
Amazon Linux (AL2)	AL2	ALAS	Sí	Sí
Amazon Linux 202 (AL2023)	AL2023	ALAS	Sí	Sí
Bottlerocket	1.7.0 y versiones posteriores	GHSA, CVE	No	Sí
CentOS Linux (CentOS)	7	CESA	Sí	Sí

Sistema operativo	Versión	Avisos de seguridad del proveedor	Compatibilidad con el análisis sin agente	Compatibilidad con el análisis basado en agentes
Debian Server (Buster)	10	DSA	Sí	Sí
Debian Server (Bullseye)	11	DSA	Sí	Sí
Debian Server (Bookworm)	12	DSA	Sí	Sí
Fedora	38	CVE	Sí	Sí
Fedora	39	CVE	Sí	Sí
OpenSUSE	15.5	CVE	Sí	Sí
Oracle Linux (Oracle)	7	ELSA	Sí	Sí
Oracle Linux (Oracle)	8	ELSA	Sí	Sí
Oracle Linux (Oracle)	9	ELSA	Sí	Sí
Red Hat Enterprise Linux (RHEL)	7	RHSA	Sí	Sí
Red Hat Enterprise Linux (RHEL)	8	RHSA	Sí	Sí

Sistema operativo	Versión	Avisos de seguridad del proveedor	Compatibilidad con el análisis sin agente	Compatibilidad con el análisis basado en agentes
Red Hat Enterprise Linux (RHEL)	9	RHSA	Sí	Sí
Rocky Linux	8	RLSA	Sí	Sí
Rocky Linux	9	RLSA	Sí	Sí
SUSE Linux Enterprise Server (SLES)	12.4	SUSE CVE	Sí	Sí
SUSE Linux Enterprise Server (SLES)	12,5	SUSE CVE	Sí	Sí
SUSE Linux Enterprise Server (SLES)	15.3	SUSE CVE	Sí	Sí
SUSE Linux Enterprise Server (SLES)	15.4	SUSE CVE	Sí	Sí
SUSE Linux Enterprise Server (SLES)	15.5	SUSE CVE	Sí	Sí
Ubuntu (Trusty)	14.04 (ESM)	USN, Ubuntu Pro	Sí	Sí
Ubuntu (Xenial)	16.04 (ESM)	USN, Ubuntu Pro	Sí	Sí

Sistema operativo	Versión	Avisos de seguridad del proveedor	Compatibilidad con el análisis sin agente	Compatibilidad con el análisis basado en agentes
Ubuntu (Bionic)	18.04 (ESM)	USN, Ubuntu Pro	Sí	Sí
Ubuntu (Focal)	20.04 (LTS)	USN	Sí	Sí
Ubuntu (Jammy)	22.04 (LTS)	USN	Sí	Sí
Ubuntu (Mantic Minotaur)	23.10	USN	Sí	Sí
Windows Server	2016	MSKB	No	Sí
Windows Server	2019	MSKB	No	Sí
Windows Server	2022	MSKB	No	Sí
macOS (Mojave)	10.14	APPLE-SA	No	Sí
macOS (Catalina)	10.15	APPLE-SA	No	Sí
macOS (Big Sur)	11	APPLE-SA	No	Sí
macOS (Monterrey)	12	APPLE-SA	No	Sí
macOS (Ventura)	13	APPLE-SA	No	Sí

Lenguajes de programación compatibles: Amazon EC2 Deep Inspection

Actualmente, Amazon Inspector admite los siguientes lenguajes de programación al escanear instancias Linux de Amazon EC2 en busca de vulnerabilidades en paquetes de software de terceros:

- Java
- JavaScript
- Python

Amazon Inspector utiliza Systems Manager Distributor para implementar el complemento que se utiliza para la inspección profunda en su instancia de Amazon EC2. Systems Manager Distributor admite los sistemas operativos que se indican en la sección Plataformas de paquetes y arquitecturas admitidas de la guía de Systems Manager. El sistema operativo de la instancia de Amazon EC2 debe ser compatible con Systems Manager Distributor y Amazon Inspector para que este pueda realizar análisis de inspección profunda.

> **Note**
>
> La inspección profunda no se admite en los sistemas operativos Bottlerocket.

Sistemas operativos compatibles: escaneo CIS

En la siguiente tabla se enumeran los sistemas operativos que Amazon Inspector admite actualmente para los escaneos CIS. La tabla también incluye la versión de referencia del CIS utilizada para realizar escaneos de ese sistema operativo.

Sistema operativo	Versión	Versión de referencia del CIS
Amazon Linux 2	AL2	2.0.0
Amazon Linux 2023	AL2023	1.0.0
Windows Server	2019	2.0.0
Windows Server	2022	2.0.0

Sistemas operativos compatibles: digitalización de Amazon ECR con Amazon Inspector

Actualmente, Amazon Inspector admite el escaneo de los siguientes sistemas operativos al escanear imágenes de contenedores en los repositorios de Amazon ECR:. En la tabla también se indica el origen de los avisos de seguridad de los proveedores para cada sistema operativo.

Sistema operativo	Versión	Avisos de seguridad del proveedor
Alpine Linux (Alpine)	3.16	Alpine SecDB
Alpine Linux (Alpine)	3.17	Alpine SecDB
Alpine Linux (Alpine)	3.18	Alpine SecDB
Alpine Linux (Alpine)	3.19	Alpine SecDB
AlmaLinux	8	ALSA
AlmaLinux	9	ALSA
Amazon Linux (AL2)	AL2	ALAS
Amazon Linux 2023 (AL2023)	AL2023	ALAS
CentOS Linux (CentOS)	7	CESA
Debian Server (Buster)	10	DSA
Debian Server (Bullseye)	11	DSA
Debian Server (Bookworm)	12	DSA
Fedora	38	CVE
Fedora	39	CVE
OpenSUSE	15.5	CVE

Sistema operativo	Versión	Avisos de seguridad del proveedor
Oracle Linux (Oracle)	7	ELSA
Oracle Linux (Oracle)	8	ELSA
Oracle Linux (Oracle)	9	ELSA
Photon OS	3	PHSA
Photon OS	4	PHSA
Photon OS	5	PHSA
Red Hat Enterprise Linux (RHEL)	7	RHSA
Red Hat Enterprise Linux (RHEL)	8	RHSA
Red Hat Enterprise Linux (RHEL)	9	RHSA
Rocky Linux	8	RLSA
Rocky Linux	9	RLSA
SUSE Linux Enterprise Server (SLES)	12.4	SUSE CVE
SUSE Linux Enterprise Server (SLES)	12.5	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.3	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.4	SUSE CVE

Sistema operativo	Versión	Avisos de seguridad del proveedor
SUSE Linux Enterprise Server (SLES)	15.5	SUSE CVE
Ubuntu (Trusty)	14.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Xenial)	16.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Bionic)	18.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Focal)	20.04 (LTS)	USN
Ubuntu (Jammy)	22.04 (LTS)	USN
Ubuntu (Mantic Minotaur)	23.10	USN

Lenguajes de programación admitidos: análisis de Amazon ECR

Actualmente, Amazon Inspector admite los siguientes lenguajes de programación al escanear imágenes de contenedores en los repositorios de Amazon ECR:

- C#
- Go
- Java
- JavaScript
- PHP
- Python
- Ruby
- Rust

Tiempos de ejecución admitidos: análisis estándar de Lambda con Amazon Inspector

El escaneo estándar de Amazon Inspector Lambda admite actualmente los siguientes lenguajes de programación para analizar funciones de Lambda en busca de vulnerabilidades en paquetes de software de terceros:

- Java
  - java8
  - java8.al2
  - java11
  - java17
- Node.js
  - nodejs12.x
  - nodejs14.x
  - nodejs16.x
  - nodejs18.x
  - nodejs20.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
- Go
  - go1.x
- Ruby
  - ruby2.7
  - ruby3.2
- .NET
  - .NET 6

Tiempos de ejecución admitidos: análisis de código de Lambda con Amazon Inspector

El escaneo de código Lambda de Amazon Inspector admite actualmente los siguientes lenguajes de programación para escanear funciones de Lambda en busca de vulnerabilidades en el código:

- Java
  - java8
  - java8.al2
  - java11
  - java17
- Node.js
  - nodejs12.x
  - nodejs14.x
  - nodejs16.x
  - nodejs18.x
  - nodejs20.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
- Ruby
  - ruby2.7
  - ruby3.2

Sistemas operativos retirados

En las siguientes tablas se indican los sistemas operativos para los que los proveedores han retirado la compatibilidad estándar. En las tablas, la columna Fecha de retirada indica la fecha en la que el proveedor retiró la compatibilidad estándar con un sistema operativo.

Anteriormente, Amazon Inspector ofrecía soporte completo para estos sistemas operativos y seguirá escaneando las instancias de Amazon EC2 y las imágenes de contenedores de Amazon ECR en las que se ejecutan. No obstante, de acuerdo con la política del proveedor, los sistemas operativos se han dejado de actualizar con parches y, en muchos casos, ya no se publican avisos de seguridad para ellos. A esto se suma que algunos proveedores eliminan los avisos de seguridad y las detecciones de sus fuentes cuando un sistema operativo afectado alcanza el final de la compatibilidad estándar. Por lo tanto, es posible que Amazon Inspector deje de generar hallazgos relacionados con CVE conocidas. Todos los hallazgos que Amazon Inspector genere con relación a un sistema operativo retirado tienen fines meramente informativos.

Como práctica de seguridad recomendada, si desea contar con la cobertura continua de Amazon Inspector, lo mejor es que empiece a utilizar una versión compatible y actualizada de un sistema operativo.

Sistemas operativos retirados: análisis de Amazon EC2

Sistema operativo	Versión	Fecha de retirada
Amazon Linux (AL1)	2012	31 de diciembre de 2021
CentOS Linux (CentOS)	8	31 de diciembre de 2021
Servidor Debian (Stretch)	9	30 de junio de 2022
Fedora	35	13 de diciembre de 2022
Fedora	36	16 de mayo de 2023
Fedora	37	5 de diciembre de 2023
OpenSUSE	15.3	1 de diciembre de 2022
OpenSUSE	15.4	7 de diciembre de 2023
openSUSE Leap (SUSE Leap)	15.2	1 de diciembre de 2021
Oracle Linux (Oracle)	6	1 de marzo de 2021
SUSE Linux Enterprise Server (SLES)	12	1 de julio de 2019

Sistema operativo	Versión	Fecha de retirada
SUSE Linux Enterprise Server (SLES)	12.1	31 de mayo de 2020
SUSE Linux Enterprise Server (SLES)	12.2	31 de marzo de 2021
SUSE Linux Enterprise Server (SLES)	12.3	30 de junio de 2022
SUSE Linux Enterprise Server (SLES)	15	31 de diciembre de 2019
SUSE Linux Enterprise Server (SLES)	15.1	31 de enero de 2021
SUSE Linux Enterprise Server (SLES)	15.2	31 de diciembre de 2021
Ubuntu (Groovy)	20,10	22 de julio de 2021
Ubuntu (Hirsute)	21,04	20 de enero de 2022
Ubuntu (Impish)	21.10	31 de julio de 2022
Ubuntu (Kinetic)	22.10	July 20, 2023
Ubuntu (Lunar Lobster)	23.04	January 25, 2024
Windows Server	2012	10 de octubre de 2023
Windows Server	2012 R2	10 de octubre de 2023

Sistemas operativos retirados: análisis de Amazon ECR

Sistema operativo	Versión	Fecha de retirada
Alpine Linux (Alpine)	3.12	1 de mayo de 2022

Sistema operativo	Versión	Fecha de retirada
Alpine Linux (Alpine)	3.13	1 de noviembre de 2022
Alpine Linux (Alpine)	3.14	May 1, 2023
Alpine Linux (Alpine)	3.15	November 1, 2023
Amazon Linux (AL1)	2012	31 de diciembre de 2021
CentOS Linux (CentOS)	8	31 de diciembre de 2021
Servidor Debian (Stretch)	9	30 de junio de 2022
Fedora	35	13 de diciembre de 2022
Fedora	36	16 de mayo de 2023
OpenSUSE	15.3	9 de diciembre de 2022
OpenSUSE	15.4	December 7, 2023
openSUSE Leap (SUSE Leap)	15.2	1 de diciembre de 2021
Oracle Linux (Oracle)	6	1 de marzo de 2021
SUSE Linux Enterprise Server (SLES)	12	1 de julio de 2019
SUSE Linux Enterprise Server (SLES)	12.1	31 de mayo de 2020
SUSE Linux Enterprise Server (SLES)	12.2	31 de marzo de 2021
SUSE Linux Enterprise Server (SLES)	12.3	30 de junio de 2022
SUSE Linux Enterprise Server (SLES)	15	31 de diciembre de 2019

Sistema operativo	Versión	Fecha de retirada
SUSE Linux Enterprise Server (SLES)	15.1	31 de enero de 2021
SUSE Linux Enterprise Server (SLES)	15.2	31 de diciembre de 2021
Ubuntu (Groovy)	20,10	22 de julio de 2021
Ubuntu (Hirsute)	21,04	20 de enero de 2022
Ubuntu (Impish)	21.10	31 de julio de 2022
Ubuntu (Kinetic)	22.10	July 20, 2023
Ubuntu (Lunar Lobster)	23.04	January 25, 2024

Desactivación de Amazon Inspector

Puede desactivar Amazon Inspector en cualquier Región de AWS con la consola de Amazon Inspector o la API. Siga las instrucciones que se indican al final de este tema para desactivar Amazon Inspector. Si desactiva todos los análisis de Amazon Inspector para una Cuenta de AWS, Amazon Inspector se desactiva automáticamente para dicha cuenta. Para obtener información acerca de la desactivación de tipos de análisis para distintos recursos, consulte Análisis automatizado de recursos con Amazon Inspector.

Una vez que Amazon Inspector se desactiva en una cuenta, se desactivan todos los tipos de análisis de dicha cuenta en esa región. Asimismo, se eliminan todas las configuraciones de análisis, reglas de supresión, filtros y hallazgos de Amazon Inspector de la cuenta en esa región.

No se le cobrará por usar Amazon Inspector mientras esté desactivado para su cuenta en esa región. Si ha desactivado Amazon Inspector, puede volver a activarlo más adelante.

> **Note**
>
> Antes de desactivar Amazon Inspector, le recomendamos que exporte los hallazgos. Para obtener más información, consulte Exportación de informes de hallazgos de Amazon Inspector.

Al desactivar los análisis de Amazon EC2 con Amazon Inspector, se eliminan las siguientes asociaciones de SSM que utiliza Amazon Inspector:

- `InspectorDistributor-do-not-delete`
- `InspectorInventoryCollection-do-not-delete`
- `InvokeInspectorSsmPlugin-do-not-delete`. Además, el complemento SSM de Amazon Inspector instalado mediante esta asociación se elimina de todos sus Windows hosts. Para obtener más información, consulte Análisis de instancias de Windows.

Requisitos previos

Según el tipo de cuenta, es posible que deba tomar las siguientes medidas adicionales antes de desactivar Amazon Inspector:

- Si tiene una cuenta independiente de Amazon Inspector, puede desactivarla en cualquier momento.
- Si tiene una cuenta de miembro en un entorno de Amazon Inspector con varias cuentas, no puede desactivar el servicio por sí mismo. Debe ponerse en contacto con el administrador delegado de la organización para que desactive el servicio.
- Si es administrador delegado, debe desasociar todas las cuentas de miembro para poder desactivar Amazon Inspector. Para obtener más información, consulte Desasociación de cuentas de miembros en Amazon Inspector.

> **Note**
>
> Al desasociar una cuenta, no se desactiva Amazon Inspector en esa cuenta. En su lugar, una cuenta de miembro desasociada se convierte en cuenta independiente.

> **Note**
>
> Al desactivar Amazon Inspector como administrador delegado, la característica de activación automática se desactiva para la organización.

Desactivación de Amazon Inspector

Console

Desactivación de Amazon Inspector

1. Abra la consola de Amazon Inspector en https://console.aws.amazon.com/inspector/v2/home.
2. Con el selector de Región de AWS de la esquina superior derecha de la página, elija la región en la que desea desactivar Amazon Inspector.
3. En el panel de navegación, elija Configuración general.
4. Elija Desactivar Inspector.
5. Cuando se le pida confirmación, introduzca desactivar en el cuadro de texto y, a continuación, elija Desactivar Inspector.
6. (Recomendado) Repita estos pasos en cada región en la que desee desactivar Amazon Inspector.

API

Ejecute la operación de la API Disable. En la solicitud, introduce los ID de cuenta que quiere desactivar y `EC2, ECR, LAMBDA` en `resourceTypes` para desactivar todos los análisis, con lo que desactivará la cuenta.

Cuotas de Amazon Inspector

La cuenta de AWS incluye las siguientes cuotas para Amazon Inspector por región.

Recurso	Valor predeterminado	Comentarios
Reglas de supresión	500	El número máximo de reglas de supresión guardadas por cuenta de AWS y por región. No puede solicitar un aumento de cuota.
Hallazgos de red de Amazon EC2	10 000	El número máximo de hallazgos de red de Amazon EC2 por cuenta de AWS. No puede solicitar un aumento de cuota.
Cuentas de miembros	10000	El número máximo de cuentas de miembros asociadas a una cuenta de administr ador delegado de Amazon Inspector. Este límite se basa en AWS Organizations. Consulte Cuotas de AWS Organizations.
Configuraciones de escaneo CIS	500	El número máximo de configuraciones de escaneo CIS.

Recurso	Valor predeterminado	Comentarios
		No puede solicitar un aumento de cuota.

Para obtener una lista de las cuotas asociadas a Amazon Inspector Classic, consulte Cuotas del servicio Amazon Inspector en la Referencia general de AWS.

Para obtener una lista de las cuotas asociadas a Organizations, consulte Cuotas del servicio Organizations en la Referencia general de AWS.

Regiones y puntos de conexión

El análisis sin agente de Amazon Inspector para Amazon EC2 se encuentra en una versión preliminar. El uso de la característica de análisis sin agente de Amazon EC2 está sujeto a la sección 2 de las Condiciones del servicio de AWS ("versiones beta y vistas previas").

Para ver las Regiones de AWS donde está disponible Amazon Inspector, consulte Puntos de conexión de Amazon Inspector en la Referencia general de Amazon Web Services.

Puntos de conexión para la API de Amazon Inspector Scan

En la siguiente tabla se muestran los puntos de conexión regionales que se pueden utilizar al llamar a la API de Amazon Inspector Scan. Al utilizar la API, debe indicar el punto de conexión y la región correspondiente a la región en la Región de AWS en la que está autenticado en este momento.

La convención de nomenclatura de los puntos de conexión de Amazon Inspector Scan es `inspector-scan.`*`region`*`.amazonaws.com`. Por ejemplo, si está autenticado en `us-west-2`, utilizaría el punto de conexión `inspector-scan.us-west-2.amazonaws.com` para llamar a la API de `inspector-scan`.

Nombre de la región	Región	Punto de conexión	Protocolo
Este de EE. UU. (Ohio)	us-east-2	inspector-scan.us-east-2.amazonaws.com inspector-scan-fips.us-east-2.amazonaws.com	HTTPS
Este de EE. UU. (Norte de Virginia)	us-east-1	inspector-scan.us-east-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
		inspector-scan-fips.us-east-1.amazonaws.com	
Oeste de EE. UU. (Norte de California)	us-west-1	inspector-scan.us-west-1.amazonaws.com inspector-scan-fips.us-west-1.amazonaws.com	HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	inspector-scan.us-west-2.amazonaws.com inspector-scan-fips.us-west-2.amazonaws.com	HTTPS
África (Ciudad del Cabo)	af-south-1	inspector-scan.af-south-1.amazonaws.com	HTTPS
Asia Pacífico (Hong Kong)	ap-east-1	inspector-scan.us-east-1.amazonaws.com	HTTPS
Asia-Pacífico (Yakarta)	ap-southeast-3	inspector-scan.ap-southeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Bombay)	ap-south-1	inspector-scan.ap-south-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Osaka)	ap-northeast-3	inspector-scan.ap-northeast-3.amazonaws.com	HTTPS
Asia-Pacífico (Seúl)	ap-northeast-2	inspector-scan.ap-northeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	inspector-scan.ap-southeast-1.amazonaws.com	HTTPS
Asia-Pacífico (Sídney)	ap-southeast-2	inspector-scan.ap-southeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	inspector-scan.ap-northeast-1.amazonaws.com	HTTPS
Canadá (centro)	ca-central-1	inspector-scan.ca-central-1.amazonaws.com	HTTPS
Europa (Fráncfort)	eu-central-1	inspector-scan.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	inspector-scan.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	inspector-scan.eu-west-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Milán)	eu-south-1	inspector-scan.eu-south-1.amazonaws.com	HTTPS
Europa (París)	eu-west-3	inspector-scan.eu-west-3.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	inspector-scan.eu-north-1.amazonaws.com	HTTPS
Europa (Zúrich)	eu-central-2	inspector-scan.eu-central-2.amazonaws.com	HTTPS
Medio Oriente (Baréin)	me-south-1	inspector-scan.me-south-1.amazonaws.com	HTTPS
América del Sur (São Paulo)	sa-east-1	inspector-scan.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Este de EE. UU.)	us-gov-este-1	inspector-scan.us-gov-east-1.amazonaws.com inspector-scan-fips.us-gov-east-1.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
AWS GovCloud (Oeste de EE.UU.)	us-gov-oeste-1	inspector-scan.us-gov-west-1.amazonaws.com inspector-scan-fips.us-gov-west-1.amazonaws.com	HTTPS

Disponibilidad de características específicas por región

En esta sección se describe la disponibilidad de las características de Amazon Inspector por Región de AWS.

Análisis de EC2 sin agente para regiones de Amazon EC2

En la siguiente tabla se muestran las Regiones de AWS en las que el análisis sin agente para Amazon EC2 está disponible actualmente.

Nombre de la región	Código de región
Este de EE. UU. (Norte de Virginia)	us-east-1
EE. UU. Oeste (Oregon)	us-west-2
Europa (Irlanda)	eu-west-1

Regiones de análisis de código de Lambda

En la siguiente tabla se muestran las Regiones de AWS en las que el análisis de código de Lambda está disponible actualmente.

Nombre de la región	Código de región
Este de EE. UU. (Norte de Virginia)	us-east-1
EE. UU. Oeste (Oregon)	us-west-2

Nombre de la región	Código de región
Este de EE. UU. (Ohio)	us-east-2
Asia Pacífico (Sídney)	ap-southeast-2
Asia-Pacífico (Tokio)	ap-northeast-1
Europa (Frankfurt)	eu-central-1
Europa (Irlanda)	eu-west-1
Europa (Londres)	eu-west-2
Europa (Estocolmo)	eu-north-1
Asia Pacífico (Singapur)	ap-southeast-1

Regiones de AWS GovCloud (US)

Para obtener la información más reciente, consulte Amazon Inspector en la Guía del usuario de AWS GovCloud (US).

Historial de documentos de la Guía del usuario de Amazon Inspector

En la siguiente tabla se describen los cambios importantes que se han realizado en la documentación desde la última versión de Amazon Inspector. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Funcionalidad actualizada	Amazon Inspector actualiza el período de retención de los hallazgos cerrados de 30 a 7 días. Para obtener más información, consulta Cómo entender los resultados de Amazon Inspector.	12 de febrero de 2024
Funcionalidad actualizada	Amazon Inspector ha agregado una nueva instrucción a la política AmazonInspector2ServiceRolePolicy. La nueva declaración permite a Amazon Inspector iniciar los escaneos CIS para su instancia.	23 de enero de 2024
Nueva política	Amazon Inspector ha añadido una nueva política, la AmazonInspector2ManagedCisPolicypolítica, que puede utilizar como parte de un perfil de instancia para permitir los escaneos de CIS en una instancia.	23 de enero de 2024

Nueva característica	Amazon Inspector actualizará ahora la duración de la redigitalización del ECR de las imágenes de los contenedores cuando las extraigas. Para cambiar la duración de la redigitalización en función de las fechas de inserción o extracción, consulte Configuración de la duración de la redigitalización del ECR.	23 de enero de 2024
Nueva característica	Amazon Inspector ahora puede ejecutar escaneos del Center for Internet Security (CIS) en instancias EC2. Para obtener más información, consulte Escaneos CIS de Amazon Inspector.	23 de enero de 2024
Nueva característica	Ahora, Amazon Inspector puede analizar imágenes de contenedores en sus canalizaciones de CI/CD. Para obtener más información, consulte Integración de CI/CD con Amazon Inspector.	30 de noviembre de 2023
Nueva política	Amazon Inspector ha añadido una nueva política que permite a Amazon Inspector analizar instantáneas de Amazon EBS desde su instancia EC2 para analizarlas sin agente. Para obtener más información sobre la política, consulte Análisis sin agente.	27 de noviembre de 2023

Nueva característica	Ahora, Amazon Inspector admite el análisis de instancias de Amazon EC2 de Linux compatibles sin agentes SSM mediante el análisis sin agente. Para obtener más información, consulte Análisis sin agente.	27 de noviembre de 2023
Nuevos recursos admitidos	Amazon Inspector ahora admite el análisis de instancias de Amazon EC2 en macOS. Consulte Sistemas operativos compatibles: análisis de Amazon EC2 para conocer las versiones de macOS compatibles.	5 de octubre de 2023
Nuevas regiones	Amazon Inspector ahora está disponible en las regiones Asia-Pacífico (Yakarta), África (Ciudad del Cabo), Asia-Pacífico (Osaka) y Europa (Zúrich).	29 de septiembre de 2023
Nueva característica	Ahora puede excluir instancias de EC2 de los análisis de Amazon Inspector con etiquetas de exclusión.	14 de septiembre de 2023

Nueva característica	Amazon Inspector ha agregado nuevos permisos que permiten a Amazon Inspector analizar las configuraciones de red de las instancias de Amazon EC2 que forman parte de los grupos de destino de Elastic Load Balancing.	31 de agosto de 2023
Nueva característica	Amazon Inspector ahora proporciona detalles sobre la inteligencia de vulnerabilidades en los hallazgos de vulnerabilidades de paquetes.	31 de julio de 2023
Funcionalidad actualizada	Amazon Inspector ha agregado nuevos permisos que permiten a los usuarios de solo lectura exportar listados de componentes de software (SBOM) de sus recursos.	29 de junio de 2023
Nueva característica	Ahora puede exportar SBOM de los recursos que analiza Amazon Inspector.	13 de junio de 2023

Nueva característica	Los análisis de código de Lambda ya están disponibles con carácter general. Se han agregado nuevas caracterí sticas que le permiten cifrar el código identificado en los hallazgos de análisis de código de Lambda. Asimismo, los análisis de código de Lambda ahora proporcio nan recomendaciones sobre cómo reescribir el código para solucionar el problema.	13 de junio de 2023
Funcionalidad actualizada	Amazon Inspector ha agregado una nueva instrucci ón a la política AmazonIns pector2ReadOnlyAccess. Las nuevas instrucciones permiten a los usuarios de solo lectura obtener detalles del estado y los hallazgos de análisis de código de Lambda de su cuenta.	2 de mayo de 2023
Nueva característica	Amazon Inspector ha agregado una herramienta de búsqueda en la base de datos de vulnerabilidades que permite comprobar si Amazon Inspector detecta una CVE específica.	1 de mayo de 2023

Funcionalidad actualizada	Amazon Inspector ha agregado nuevos permisos a la política AmazonInspector2ServiceRolePolicy que permiten a Amazon Inspector crear canales vinculados a servicios de AWS CloudTrail en su cuenta al activar los análisis de Lambda. Esto permite a Amazon Inspector supervisar CloudTrail los eventos de tu cuenta.	30 de abril de 2023
Funcionalidad actualizada	Amazon Inspector ha agregado una nueva instrucción a la política AmazonInspector2FullAccess. La nueva instrucción permite a los usuarios obtener detalles de los hallazgos de vulnerabilidades de código a partir de los análisis de código de Lambda.	17 de abril de 2023
Funcionalidad actualizada	Amazon Inspector ha agregado una nueva instrucción a la política AmazonInspector2ServiceRolePolicy. La nueva declaración permite a Amazon Inspector enviar información a Amazon EC2 Systems Manager sobre las rutas personalizadas que ha definido para la inspección profunda de Amazon EC2.	17 de abril de 2023

Nueva característica	Amazon Inspector añade soporte adicional para las instancias EC2 de Linux mediante la inspección profunda de Amazon Inspector , que analiza las instancias en busca de vulnerabilidades de paquetes en paquetes de lenguajes de programación de aplicaciones.	17 de abril de 2023
Funcionalidad actualizada	Amazon Inspector ha agregado una nueva instrucción a la política AmazonInspector2ServiceRolePolicy. Las nuevas declaraciones permiten a Amazon Inspector solicitar escaneos del código del desarrollador en AWS Lambda las funciones y recibir datos de escaneo de Amazon CodeGuru Security. Además, Amazon Inspector ha agregado permisos para revisar las políticas de IAM. Amazon Inspector utiliza esta información para analizar las funciones de Lambda en busca de vulnerabilidades de código.	28 de febrero de 2023

Nueva característica	Amazon Inspector ha agregado compatibilidad adicional para funciones de Lambda en forma de análisis de código de Lambda, que analizan el código del desarrollador de las funciones de Lambda en busca de vulnerabilidades de seguridad.	28 de febrero de 2023
Funcionalidad actualizada	Amazon Inspector ha agregado una nueva instrucción a la política AmazonInspector2ServiceRolePolicy. La nueva declaración permite a Amazon Inspector recuperar información CloudWatch sobre cuándo se invocó una AWS Lambda función por última vez. Utiliza esta información para centrar los escaneos en las funciones Lambda de su entorno que han estado activas durante los últimos 90 días.	20 de febrero de 2023

Funcionalidad actualizada	Amazon Inspector ha agregado una nueva instrucción a la política AmazonInspector2ServiceRolePolicy. La nueva instrucción permite a Amazon Inspector obtener información acerca de las funciones de AWS Lambda. Amazon Inspector utiliza esta información para analizar las funciones de Lambda en busca de vulnerabilidades de seguridad.	28 de noviembre de 2022
Nueva característica	Amazon Inspector ha agregado compatibilidad para los análisis de funciones de AWS Lambda.	28 de noviembre de 2022
Contenido actualizado	Se han agregado procedimientos, ejemplos de políticas y consejos sobre cómo exportar informes de hallazgos de Amazon Inspector a un bucket de Amazon Simple Storage Service (Amazon S3).	14 de octubre de 2022
Nuevo contenido	Se ha agregado información acerca de la evaluación de la cobertura de Amazon Inspector para el entorno de AWS mediante la consola de Amazon Inspector. Esta información incluye descripciones de los valores de Estado para cada recurso del entorno.	7 de octubre de 2022

Nueva característica	Amazon Inspector ahora proporciona más información sobre cómo corregir vulnerabilidades de paquetes. Se han agregado nuevos campos a los detalles de los hallazgos. Los nuevos campos proporcionan contexto sobre si hay una corrección disponible en un paquete de actualizaciones. Si la hay, en la sección Solución sugerida del hallazgo se muestran los comandos que puede ejecutar para aplicarla.	2 de septiembre de 2022
Funcionalidad actualizada	Amazon Inspector ha agregado una nueva acción a la política AmazonInspector2ServiceRolePolicy. La nueva acción permite a Amazon Inspector describir las ejecuciones de asociaciones de SSM. Además, Amazon Inspector ha agregado ámbitos de aplicación de recursos adicionales que permiten a Amazon Inspector crear, actualizar, eliminar e iniciar asociaciones de SSM con documentos de SSM propiedad de `AmazonInspector2` .	31 de agosto de 2022

Nueva característica	Amazon Inspector ahora admite análisis de instancias de Windows. Amazon Inspector ahora puede analizar instancias administradas en SSM que ejecutan sistemas operativos Windows compatibles. Los escaneos de los Windows hosts los realiza el complemento SSM de Amazon Inspector, que se instala e invoca mediante nuevas asociaciones de SSM creadas automáticamente por Amazon Inspector.	31 de agosto de 2022
Funcionalidad actualizada	Amazon Inspector ha actualizado el ámbito de aplicación de recursos de la política AmazonInspector2ServiceRolePolicy para permitir que Amazon Inspector pueda obtener datos de inventario de software en otras particiones de AWS.	12 de agosto de 2022
Funcionalidad actualizada	En la política AmazonInspector2ServiceRolePolicy, Amazon Inspector ha reestructurado el ámbito de aplicación de recursos de las acciones para permitir que Amazon Inspector pueda crear, eliminar y actualizar asociaciones de SSM.	10 de agosto de 2022

Nueva característica	Amazon Inspector ahora admite la modificación del parámetro de duración de los análisis repetidos y automatizados de ECR. Este parámetro determina durante cuánto tiempo Amazon Inspector supervisa continuamente las imágenes insertadas en repositorios. Cuando una imagen es más antigua que la duración del análisis, Amazon Inspector deja de analizar la imagen y cierra todos los hallazgos relacionados con esta. La duración de los análisis repetidos y automatizados de ECR se establece durante toda la vigencia del servicio en las nuevas cuentas. En cuentas que ya estaban creadas, este valor era de 30 días, aunque ahora puede elegir si desea que los análisis duren 30 días, 180 días o por toda la vigencia del servicio.	25 de junio de 2022
Nueva funcionalidad	Amazon Inspector ha agregado una política administrada de AWS, la política AmazonInspector2ReadOnlyAccess, para permitir el acceso de solo lectura a la funcionalidad de Amazon Inspector.	21 de enero de 2022

Disponibilidad general	Esta es la versión pública inicial de la Guía del usuario de Amazon Inspector.	29 de noviembre de 2021

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

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.