Guía del usuario

AWS Audit Manager

AWS Audit Manager: Guía del usuario

Table of Contents

¿Qué es AWS Audit Manager?

Le damos la bienvenida a la Guía del usuario de AWS Audit Manager.

AWS Audit Manager permite auditar continuamente el uso de AWS y así simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector. Audit Manager automatiza la recopilación de evidencias para que pueda evaluar más fácilmente si sus políticas, procedimientos y actividades (también conocidas como controles) son eficaces. Llegado el momento de una auditoría, Audit Manager le ayuda a gestionar las revisiones de sus controles por parte de las personas interesadas. Esto significa que puede crear informes listos para la auditoría con mucho menos esfuerzo manual.

Audit Manager proporciona marcos prediseñados que estructuran y automatizan las evaluaciones para normas o reglamentos de cumplimiento determinados. Estos marcos incluyen una colección prediseñada de controles con descripciones y procedimientos de prueba. Asimismo, se agrupan según los requisitos de la norma o reglamento de cumplimiento en cuestión. También puede personalizar los marcos y los controles para las auditorías internas de acuerdo con sus requisitos específicos.

Puede crear evaluaciones desde cualquier marco. Al crear una evaluación, Audit Manager ejecuta automáticamente las evaluaciones de los recursos. Estas recopilan datos tanto para Cuenta de AWS como para los servicios que defina como incluidos en la auditoría. Los datos que se recopilan se transforman automáticamente en evidencias aptas para la auditoría. Luego, se agregan a los controles pertinentes para mostrar, así, el cumplimiento en materia de seguridad, gestión de cambios, continuidad empresarial y licencias de software. El proceso de recopilación de evidencias es continuo y comienza cuando se crea la evaluación. Una vez completada la auditoría, puede detener la recopilación de evidencias si ya no necesita Audit Manager para ello. Para hacerlo, cambie el estado de la evaluación a inactiva.

Características de Audit Manager

Con AWS Audit Manager, puede realizar las siguientes tareas:

- Inicio rápido: cree su primera evaluación eligiendo la opción que mejor se adapte a sus necesidades de entre una galería de marcos prediseñados diseñados una variedad de normas y reglamentos de cumplimiento. A continuación, puede iniciar la recopilación automática de evidencias para auditar su uso de Servicio de AWS.

- Carga y gestión de evidencias de entornos híbridos o multinube: además de las evidencias que Audit Manager recopila de su entorno de AWS, también puede cargar y gestionar las evidencias de su entorno local o multinube de forma centralizada.
- Compatibilidad con normas y reglamentos de cumplimiento estándares: elija uno de los marcos estándar de AWS Audit Manager. Estos marcos proporcionan asignaciones de control predefinidas para las normas y reglamentos de cumplimiento más habituales, como, por ejemplo, el CIS Foundation Benchmark, el PCI DSS, el RGPD, la HIPAA, el SOC 2, la GxP y las mejores prácticas operativas. AWS
- Supervisión de evaluaciones activas: consulte los datos de análisis de sus evaluaciones activas e identifique rápidamente las evidencias no conformes que deban corregir gracias al panel de Audit Manager.
- Búsqueda de evidencias: utilice la característica de búsqueda de evidencias para encontrar rápidamente las pruebas que sean relevantes para su consulta de búsqueda. Puede generar informes de evaluación a partir de los resultados de la búsqueda o exportar los resultados de la búsqueda en formato CSV.
- Creación de controles personalizados: cree su propio control desde cero o personalice un control existente adaptándolo a sus necesidades. También puede usar la característica de los controles personalizados para crear preguntas de evaluación de riesgos y almacenar las respuestas a esas preguntas como evidencias manuales.
- Personalización de los marcos: cree sus propios marcos con controles estándar o personalizados en función de sus necesidades para las auditorías internas.
- Marcos personalizados compartidos: comparta sus marcos personalizados de Audit Manager con otra Cuenta de AWS o reprodúzcalos en otra Región de AWSdesde su propia cuenta.
- Compatibilidad con la colaboración entre equipos: delegue los conjuntos de controles a expertos en la materia que puedan revisar las evidencias relacionadas, añadir comentarios y actualizar el estado de cada control.
- Creación de informes para la auditoría: genere informes de evaluación que resuman las evidencias relevantes recopiladas para la auditoría y enlacen a las carpetas que contienen las evidencias detalladas.
- Garantía de la integridad de las evidencias: guarde las evidencias en un lugar seguro donde no se modifiquen.

> **Note**
>
> AWS Audit Manager ayuda a recopilar evidencias relevantes para verificar el cumplimiento de normas y reglamentos de cumplimiento específicos. Sin embargo, no evalúa el cumplimiento en sí mismo. Por lo tanto, es posible que las evidencias recopiladas mediante AWS Audit Manager no incluyan toda la información sobre su uso de AWS que se necesita para las auditorías. AWS Audit Manager no sustituye a los asesores legales ni a los expertos en cumplimiento.

Precios de Audit Manager

Para obtener más información sobre los precios, consulte Precios de AWS Audit Manager.

¿Es la primera vez que usa Audit Manager?

Si es la primera vez que usa Audit Manager, le recomendamos que comience con las páginas siguientes:

1. Conceptos y terminología de AWS Audit Manager: conozca los conceptos y términos clave que se utilizan en Audit Manager, como las evaluaciones, los marcos y los controles.
2. Cómo recopila AWS Audit Manager las evidencias: conozca cómo Audit Manager recopila las evidencias para evaluar los recursos.
3. Configuración: conozca los requisitos de configuración de Audit Manager.
4. Introducción: siga un tutorial para crear su primera evaluación de Audit Manager.
5. Información sobre la API de AWS Audit Manager: familiarícese con las acciones y los tipos de datos de la API de Audit Manager.

Más recursos de Audit Manager

Consulte estos recursos para obtener más información sobre Audit Manager.

- Recopile evidencias y gestione los datos de auditoría mediante AWS Audit Manager
- Configure manualmente una evaluación de Audit Manager personalizada desde AWS Workshops

- Integre el modelo de tres líneas (parte 2): transforme los paquetes de conformidad de AWS Config en evaluaciones de AWS Audit Manager siguiendo el la entrada sobre administración y gobierno en AWS

Conceptos y terminología de AWS Audit Manager

En este tema se explican algunos de los conceptos clave que debe conocer para comenzar a utilizar AWS Audit Manager.

A

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Evaluaciones

Recopile evidencias relevantes para las auditorías automáticamente con las evaluaciones de Audit Manager.

Las evaluaciones se basan en marcos, es decir agrupaciones de controles relacionados con las auditorías. En función de los requisitos de su empresa, puede crear evaluaciones a partir de marcos estándares o personalizados. Los marcos estándar contienen conjuntos de controles prediseñados que con arreglo a una norma o reglamento de cumplimiento específico. Los marcos personalizados, en cambio, contienen controles que puede personalizar y agrupar según sus requisitos de auditoría interna. Si utiliza un marco como punto de partida, puede crear una evaluación que especifique las Cuentas de AWS y los servicios que desea incluir en la auditoría.

Al crear una evaluación, Audit Manager comienza a evaluar los recursos de sus Cuentas de AWS y servicios automáticamente en función de los controles que se definen en el marco. A continuación, recopila las evidencias relevantes y las convierte a un formato fácil de usar para los auditores. Una vez hecho esto, agrega las evidencias a los controles de evaluación. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas recopiladas y, a continuación, añadirlas a un informe de evaluación. Este informe de evaluación le ayuda a demostrar que sus controles funcionan según lo previsto.

La recopilación de evidencias es un proceso continuo que comienza cuando se crea la evaluación. Puede detener la recopilación de evidencias, o bien cambiando el estado de la evaluación a inactiva, o bien en el nivel de control. Para ello, puede cambiar el estado de un control de su evaluación en concreto a inactivo.

Para obtener instrucciones acerca de cómo crear y administrar las evaluaciones, consulte Evaluaciones en AWS Audit Manager.

Informes de evaluación

Los informes de evaluación son documentos finalizados que se generan a partir de una evaluación de Audit Manager. Estos informes resumen las evidencias relevantes recopilada para la auditoría, y están enlazados con las carpetas de evidencias pertinentes. Estas carpetas se nombran y organizan de acuerdo con los controles que se especifican en cada evaluación. Puede revisar qué evidencias recopila Audit Manager para cada evaluación y decidir cuáles desea incluir en el informe de evaluación.

Para más información acerca de estos informes, consulte Informes de evaluación. Para información sobre cómo generar un informe de evaluación, consulte Generación de informes de evaluación.

Destino de los informes de evaluación

El destino de los informes de evaluación es el bucket S3 predeterminado en el que Audit Manager guarda los informes de evaluación. Para obtener más información, consulte Destino del informe de evaluación (opcional).

Auditoría

Las auditorías son exámenes independientes de los activos, las operaciones o la integridad empresarial de su organización. Las auditorías de tecnología de la información (TI) examinan específicamente los controles de los sistemas de información de su organización. El objetivo de estas auditorías es determinar si los sistemas de información protegen los activos, funcionan de manera eficaz y mantienen la integridad de los datos. Todo esto es importante para cumplir con los requisitos reglamentarios exigidos por las normas o reglamentos de cumplimiento.

Responsable de la auditoría

El término responsable de la auditoría tiene dos significados diferentes según el contexto.

En el contexto de Audit Manager, el responsable de una auditoría es un usuario o rol que gestiona una evaluación y sus recursos relacionados. Se encarga de la creación de evaluaciones, la revisión de las evidencias y la generación de informes de evaluación. Audit Manager es un servicio colaborativo y los responsables de auditorías se benefician cuando otras partes interesadas participan en sus evaluaciones. Por ejemplo, puede añadir a otros responsables de la auditoría a su evaluación para compartir las tareas de administración. Además, si es responsable

de una auditoría y necesita ayuda para interpretar las evidencias recopiladas para un control, puede delegar ese conjunto de controles a otra parte interesada que tenga experiencia en la materia. En ese caso, la persona se conoce como persona delegada.

En términos comerciales, el responsable de una auditoría es quien coordina y supervisa las iniciativas de preparación para la auditoría de su empresa y presenta las evidencias al auditor. Por lo general, se trata de un profesional de la gobernanza, el riesgo y el cumplimiento (GRC). Puede ser. por ejemplo, un responsable de cumplimiento o de protección de datos del RGPD. Los profesionales del GRC tienen la experiencia y la autoridad adecuadas para gestionar la preparación de las auditorías. Más específicamente, comprenden los requisitos de cumplimiento y pueden analizar, interpretar y preparar los datos de los informes. Sin embargo, otras funciones empresariales también pueden ser Audit Manager del responsable de una auditoría; no solo los profesionales de GRC asumen esta función. Por ejemplo, puede optar por que un experto técnico de uno de los siguientes equipos configure y gestione las evaluaciones de Audit Manager:

- SecOps
- TI y DevOps
- Centro de operaciones de seguridad/respuesta a incidentes
- Equipos similares que poseen, desarrollan, corrigen e implementan activos en la nube y comprenden la infraestructura de nube de su organización

La persona elegida como responsable de la auditoría en su evaluación de Audit Manager dependerá en gran medida de su organización y también de cómo se estructuren las operaciones de seguridad y de las características específicas de la auditoría. En Audit Manager, una misma persona puede asumir el rol de responsable de la auditoría en una evaluación y, el de delegado, en otra.

Independientemente de cómo utilice Audit Manager, puede gestionar la separación de funciones en su organización utilizando la persona propietaria o delegada de la auditoría y otorgando políticas de IAM específicas a cada usuario. Mediante este enfoque de dos pasos, Audit Manager garantiza que usted tenga el control total sobre todos los aspectos específicos de cada evaluación. Para más información, consulte las políticas recomendadas para los usuarios en AWS Audit Manager.

C

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Registros de cambios

Para cada control de una evaluación, Audit Manager captura los registros de cambios con el objetivo de realizar un seguimiento de la actividad de los usuarios en dicho control. A continuación puede revisar un registro de auditoría de las actividades relacionadas con un control específico. Para más información sobre las actividades de los usuarios que se capturan en los registros de cambios, consulte Pestaña del registro de cambios.

Conformidad en la nube

La conformidad con la nube es el principio general según el cual los sistemas suministrados en la nube deben cumplir con los estándares que se aplican a los clientes de la nube.

Regulación del cumplimiento

Los reglamentos de cumplimiento son leyes, normas órdenes de otro tipo prescritas por una autoridad, normalmente para regular una conducta. Un ejemplo de ello es el RGPD.

Estándares de conformidad

Los estándares de conformidad son un conjunto estructurado de directrices que detallan los procesos de una organización para mantener la conformidad con las normas, especificaciones o legislación establecidas. Algunos ejemplos de ello son el PCI DSS y la HIPAA.

Control

Los controles son salvaguardias o medidas que se prescriben para un sistema de información o una organización. Los controles están diseñados para proteger la confidencialidad, integridad y disponibilidad de su información y para cumplir con un conjunto de requisitos de seguridad definidos previamente. Garantizan que sus recursos funcionan según lo previsto, que sus datos son fiables y que su organización cumple con las leyes y reglamentos aplicables.

En Audit Manager, los controles también pueden ser preguntas en un cuestionario de evaluación de riesgos para proveedores. En ese caso, se trata de una pregunta específica que solicita información sobre la postura de seguridad y cumplimiento de una organización.

Los controles recopilan evidencias de forma continua cuando están activos en sus evaluaciones de Audit Manager. También puede agregar evidencias de forma manual a cualquier control. Cada evidencia se convierte en un registro que le permite mostrar el cumplimiento de los requisitos del control.

Hay dos tipos de control en Audit Manager:

- Los controles estándar, que son los controles prediseñados asociados a un marco concreto de Audit Manager. Los controles estándar serán de utilidad para preparar las auditorías en relación con diversas normas y reglamentos de conformidad.
- Los controles personalizados, que son los que usted define como usuario de Audit Manager. Estos controles le ayudarán a cumplir los requisitos de conformidad específicos de las auditorías internas o las evaluaciones de riesgos de los proveedores.

Para más información, consulte los Ejemplos de controles en AWS Audit Manager. Para obtener instrucciones sobre cómo crear y configurar los controles, consulte Biblioteca de control.

Dominios de control

Piense en los dominios de control como una categoría general de controles que no es específica de ningún marco en particular. Las agrupaciones de dominios de control son una de las funciones más potentes del panel de control de Audit Manager. Audit Manager destaca los controles de sus evaluaciones que contienen evidencias no conformes y los agrupa por dominio de control. Esto le permite centrar sus esfuerzos de remediación en ámbitos temáticos específicos mientras se prepara para una auditoría.

> **Note**
>
> Tenga en cuenta que los dominios no son conjuntos de controles. Los conjuntos de controles son agrupaciones de controles específicas de un marco, que suelen definir los organismos reguladores. Por ejemplo, el marco PCI DSS tiene un conjunto de controles denominado “Requisito 8: identificar y autenticar el acceso a los componentes del sistema”. Este conjunto de control pertenece al dominio de control de la gestión de identidad y acceso.

Audit Manager clasifica los controles en los dominios de control siguientes.

Nombre de dominio de control	Descripción de lo que rigen los controles
Planificación de contingencia y continuidad del negocio	Cómo se establecen los procesos que protegen las operaciones comerciales críticas de los efectos de las principales interrupciones del sistema y la red.

Nombre de dominio de control	Descripción de lo que rigen los controles
Administración de cambios	Cómo se prueban, aprueban, implementan y documentan los cambios en su infraestructura de nube.
Seguridad y privacidad de datos	Cómo protege la privacidad, la disponibilidad y la integridad de sus datos.
Gestión del desarrollo y la configuración	Cómo se mantiene la infraestructura de la nube en el estado deseado y coherente.
Gobierno y supervisión	Cómo concuerda el uso de la computación en la nube con sus obligacio nes legales, reglamentarias y éticas.
Administración de identidades y accesos	Cómo se asegura de que los usuarios correctos tengan el acceso adecuado a sus recursos tecnológicos.
Administración de incidentes	Cómo se establecen las responsabilidades y los procedimientos que garantizan una respuesta rápida y eficaz a los incidentes de seguridad.
Registro y monitoreo	Cómo se revisa la actividad de los usuarios para detectar indicios de que se ha intentado o realizado una actividad no autorizada.
Administrador de red	Cómo se administra y opera la red de datos mediante un sistema de administración de red.
Administración de personal	Cómo se evalúan y gestionan los riesgos de seguridad del personal a nivel organizativo.
Seguridad física	Cómo se detectan y previenen los problemas de seguridad física en sus instalaciones.
Gestión de riesgos	Cómo se evalúan los posibles riesgos y pérdidas y cómo se reducen o eliminan dichas amenazas.

Nombre de dominio de control	Descripción de lo que rigen los controles
Gestión de la cadena de suministro	Cómo se identifican, evalúan y mitigan los riesgos asociados a los productos, proveedores y cadenas de suministro de TI.
Administración de los dispositivos de los usuarios	Cómo se reduce el riesgo de que el hardware de TI de sus empleados se pierda, se dañe o se esté en peligro.
Gestión de vulnerabilidades	Cómo se definen, evalúan y corrigen todas las vulnerabilidades conocidas de los activos de su infraestructura de nube.

D

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Origen de datos

Audit Manager utiliza un origen de datos para recopilar evidencias para los controles. La terminología siguiente describe qué es un origen de datos y cómo funciona.

- Los tipos de origen de datos definen el lugar desde el cual Audit Manager recopila las evidencias para los controles. Si carga sus propias evidencias, el tipo de origen de datos es Manual. Si Audit Manager recopila las evidencias en su nombre, el tipo de origen de datos es AWS Security Hub, AWS ConfigAWS CloudTrail, o llamadas a la API de AWS. La API Audit Manager hace referencia a un tipo de origen de datos como SourceType (singular) o ControlSources (plural).
- Una asignación es una palabra clave específica relacionada con un tipo de origen de datos. Por ejemplo, puede ser el nombre de un evento de CloudTrail o un nombre de AWS Config. En la API de Audit Manager esto se conoce como SourceKeyword (singular) o ControlMappingSources (plural).
- El nombre de un origen de datos es la denominación que se da a un origen de datos. En otras palabras, el nombre de un origen de datos etiqueta la combinación de un tipo de origen de datos y una asignación. En el caso de los controles estándar, Audit Manager proporciona un nombre de origen de datos predeterminado (como origen de datos 1 y origen de datos 2). No obstante, puede elegir su propio nombre de origen de datos para los controles personalizados.

Esto puede ayudarle a distinguir entre varias asignaciones que pertenecen al mismo tipo de origen de datos. La API Audit Manager hace referencia al nombre de los orígenes de datos como SourceName.

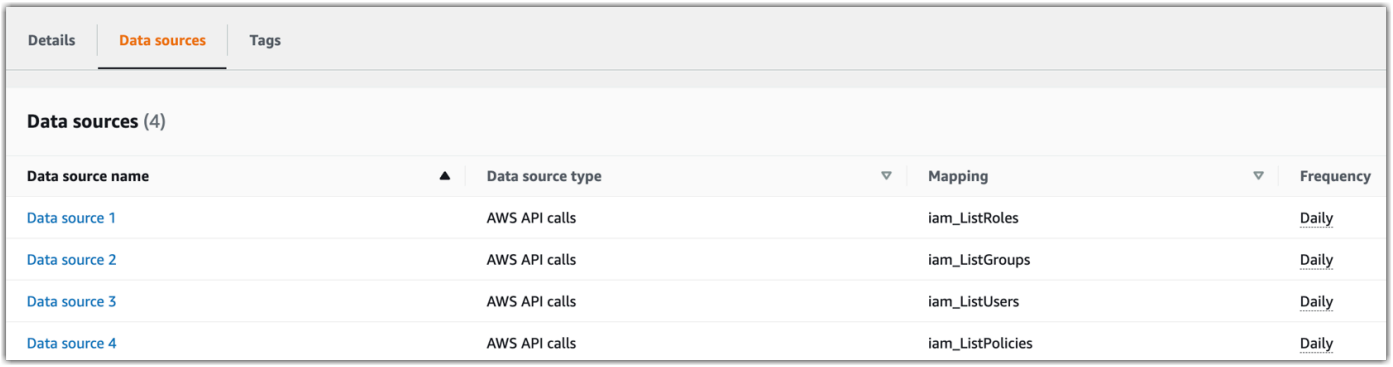
Un único control puede tener varios tipos de orígenes de datos y diferentes asignaciones. Por ejemplo, un control puede recopilar evidencias de varios tipos de origen de datos (como AWS Config y Security Hub). Es posible que otro control tenga AWS Config como único tipo de origen de datos, con varias reglas de AWS Config como asignaciones.

En la tabla siguiente se enumeran los tipos de origen de datos automatizados y se muestran ejemplos de algunas de las asignaciones correspondientes.

Data source type	Descripción	Ejemplo de asignación
AWS Security Hub	Utilice este tipo de origen de datos para capturar instantáneas del estado de seguridad de sus recursos. Audit Manager usa el nombre de un control de Security Hub como palabra clave de la asignación e informa del resultado del control de seguridad de dicha regla directamente desde Security Hub.	`1.1 – Avoid the use of the "root" account`
AWS Config	Utilice este tipo de origen de datos para capturar instantáneas del estado de seguridad de sus recursos. Audit Manager usa el nombre de una regla de AWS Config como palabra clave de asignación e informa el resultado de la verificación de dicha regla directamente desde AWS Config.	`EC2_INSTANCE_MANAGED_BY_SSM`

Data source type	Descripción	Ejemplo de asignación
AWS CloudTrail	Utilice este tipo de origen de datos para realizar un seguimiento de la actividad de un usuario específica que sea necesaria en la auditoría. Audit Manager usa el nombre de un evento de CloudTrai l como palabra clave de asignación y recopila la actividad relacionada del usuario desde sus registros de CloudTrail.	`CreateAccessKey`
Llamadas a la API de AWS	Utilice este tipo de origen de datos para tomar una instantánea de la configura ción de sus recursos mediante una llamada a la API a un recurso de Servicio de AWS en concreto. Audit Manager usa el nombre de la llamada a la API como palabra clave de asignación y recopila la respuesta de la API.	`ec2_DescribeSecuri tyGroups`

La siguiente imagen muestra ejemplos de diferentes orígenes de datos, tal y como se ve en la consola de Audit Manager.



> **Note**
>
> Aunque algunos tipos de fuentes de datos son Servicios de AWS, el tipo de origen de datos es diferente al de un servicio incluido. Para más información, consulte ¿Cuál es la diferencia entre un servicio incluido y un tipo de origen de datos? en el apartado de solución de problemas de esta guía.

Delegados

Los delegados son un usuarios de AWS Audit Manager con permisos limitados y suelen tener experiencia empresarial o técnica especializada. Estos conocimientos pueden estar relacionados, por ejemplos, con las políticas de retención de datos, los planes de formación, la infraestructura de red o la gestión de identidades. Los delegados ayudan a los responsables de la auditoría a revisar las evidencias recopiladas para comprobar si hay controles que estén dentro de su área de especialización. Pueden revisar los conjuntos de controles y las evidencias relacionadas con estos, añadir comentarios, cargar evidencias adicionales y actualizar el estado de cada una de las evaluaciones que les asigne para revisar.

Los responsables de las auditorías asignan conjuntos de controles específicos a los delegados, no a evaluaciones completas. En consecuencia, los delegados tienen acceso limitado a las evaluaciones. Para obtener instrucciones acerca de cómo delegar un conjunto de controles, consulte Delegación en AWS Audit Manager.

E

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Evidencias

Las evidencias son registros que contienen la información necesaria para demostrar el cumplimiento de los requisitos de una evaluación. Las evidencias pueden ser, por ejemplo, las actividades de cambio invocadas por los usuarios o instantáneas de la configuración del sistema.

Hay dos tipos de evidencia principales en Audit Manager: las evidencias automatizadas y evidencias manuales.

- Las evidencias automatizadas son el tipo de información que Audit Manager recopila automáticamente. Esto incluye las siguientes tres categorías de evidencias automatizadas:
  - Las verificaciones de conformidad, es decir el resultado de una verificación de conformidad se captura a partir de AWS Security Hub, AWS Config o de ambas fuentes. Son ejemplos de comprobaciones de conformidad los resultados de los controles de seguridad de Security Hub para las comprobaciones de PCI DSS y las evaluaciones de AWS Config de reglas para un control de HIPAA. Para más información, consulte las AWS Configreglas compatibles AWS Audit Manager y AWS Security Hub los controles compatibles con AWS Audit Manager.
  - La actividad de los usuarios que modifica la configuración de los recursos se captura desde los registros de CloudTrail conforme se produce. Entre los ejemplos de actividades de los usuarios destacan las actualizaciones de la tabla de enrutamiento, los cambios en la configuración de la copia de seguridad de las instancias de Amazon RDS o en la política de cifrado de buckets de S3. Para más información, consulte los AWS CloudTrailnombres de eventos compatibles con AWS Audit Manager.
  - Los datos de configuración se refieren a la captura una instantánea de la configuración de los recursos directamente de Servicio de AWS de forma diaria, semanal o mensual. Los ejemplos de instantáneas de configuración incluyen las listas de rutas para las tablas de enrutamiento de VPC, la configuración de las copias de seguridad de instancias de Amazon RDS y la política de cifrado de buckets de S3. Para más información sobre las acciones de la API compatibles, consulteAWS Audit Manager.
- Las evidencias manuales son las que usted mismo añade a Audit Manager. Hay tres maneras de añadir sus propias evidencias:
  - Importar un archivo desde Amazon S3
  - Cargar un archivo desde el navegador
  - Escribir el texto de respuesta a las preguntas de evaluación de riesgos.

  Para obtener más información, consulte Carga manual de evidencias en AWS Audit Manager.

La recopilación automática de evidencias comienza cuando se crea una evaluación. Se trata de un proceso continuo, durante el cual Audit Manager recopila evidencias a diferentes frecuencias según el tipo de evidencias y el origen de datos subyacente. Para más información sobre la recopilación de evidencias, consulte ¿Cómo recopila AWS Audit Manager las evidencias?. Para obtener instrucciones acerca de cómo revisar las evidencias de una evaluación, consulte Revisión de las evidencias de una evaluación.

Métodos de recopilación de evidencias

Las evaluaciones pueden recopilar evidencias de dos maneras distintas.

- Los controles automatizados recopilan evidencias de los orígenes de AWS datos automáticamente. Las evidencias automatizadas pueden ayudarle a demostrar el cumplimiento total o parcial de las evaluaciones.
- Las evaluaciones manuales requieren que cargue sus propias evidencias para demostrar el cumplimiento de las mismas.

> **Note**
>
> Puede agregar evidencias manuales a cualquier evaluación automatizada. En muchos casos, es necesaria una combinación de evidencias automatizadas y manuales para demostrar el pleno cumplimiento de una evaluación. Si bien Audit Manager puede proporcionar evidencias automatizadas útiles y relevantes, es posible que algunas de ellas solo demuestren un cumplimiento parcial. En este caso, puede complementar las evidencias automatizadas de proporciona Audit Manager con sus propias evidencias. Por ejemplo:
>
> - El AWSmarco de mejores prácticas de IA generativa contiene un control denominado "`Error analysis`". Deberá identificar cuándo se detectan imprecisiones en el uso del modelo y realizar un análisis exhaustivo de los errores para comprender las causas de los mismos y tomar las medidas correctivas apropiadas.
> - Para respaldar este control, Audit Manager recopila evidencias automatizadas que muestran si las alarmas de CloudWatch están habilitadas para la Cuenta de AWS donde se está ejecutando la evaluación. Puede utilizar estas evidencias para demostrar el cumplimiento parcial de la evaluación comprobando que sus alarmas y comprobaciones están configuradas correctamente.
> - Para demostrar el pleno cumplimiento, puede complementar las evidencias automatizadas con evidencias manuales. Por ejemplo, puede subir una política o un procedimiento que muestre su proceso de análisis de errores, sus umbrales

de escalado y generación de informes, y los resultados del análisis de la causa principal. Puede utilizar las evidencias de este manual para demostrar que hay políticas establecidas y que se tomaron medidas correctivas cuando se le solicitó.

Para ver un ejemplo más detallado, consulte Controles con orígenes de datos mixtos.

Destinos de exportación

Los destinos de exportación son los buckets S3 predeterminados, donde Audit Manager guarda los archivos que exporta desde el buscador de evidencias. Para obtener más información, consulte Destino de exportación (opcional).

F

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Marcos

Los marcos de Audit Manager son archivos que se utilizan para estructurar y automatizar las evaluaciones para un estándar o un principio de gobierno de riesgos específicos. Ayudan a asignar los recursos de AWS a los requisitos de un control e incluyen varios prediseñados o definidos por el cliente. Los conjuntos de marcos incluyen descripciones y procedimientos de prueba para cada control. Los controles se organizan y agrupan en función de los requisitos de una norma o reglamento de cumplimiento en concreto. Son ejemplos de ello el PCI, el DSS y el RGPD.

Hay dos tipos de estructuras en Audit Manager:

- Los marcos estándar son marcos prediseñados que se basan en las mejores prácticas de AWS para diversas normas y reglamentos de cumplimiento. Utilícelos para facilitar la preparación de la auditoría.
- Los marcos personalizados son los que usted define como usuario de Audit Manager. Le pueden ser de utilidad para preparar auditorías de acuerdo según sus requisitos específicos de cumplimiento o control de riesgos.

Para obtener instrucciones acerca de cómo crear y administrar marcos, consulte Biblioteca de marcos.

> **Note**
>
> AWS Audit Manager ayuda a recopilar evidencias relevantes para verificar el cumplimiento de normas y reglamentos de cumplimiento específicos. Sin embargo, no evalúa el cumplimiento en sí mismo. Por lo tanto, es posible que las evidencias recopiladas mediante AWS Audit Manager no incluyan toda la información sobre su uso de AWS que se necesita para las auditorías. AWS Audit Manager no sustituye a los asesores legales ni a los expertos en cumplimiento.

Marcos compartidos

Puede usar la característica de uso compartido de los marcos de trabajo personalizados de Audit Manager para compartir rápidamente sus marcos personalizados en todas las Cuentas de AWS y regiones. Para compartir marcos personalizados, debe crear una solicitud de uso compartido. El destinatario de la solicitud de uso compartido tendrá entonces 120 días para aceptarla o rechazarla. Una vez aceptada, Audit Manager replicará el marco de trabajo personalizado compartido en su biblioteca de marcos. Además de replicar el marco de trabajo personalizado, Audit Manager también replicará todos los conjuntos de controles personalizados y los controles que formen parte de ese marco. Posteriormente, dichos controles personalizados se agregan a la biblioteca de controles del destinatario. Audit Manager no replica los marcos o controles estándar. Esto se debe a que estos recursos ya están disponibles de forma predeterminada en cada cuenta y región.

R

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Recursos

Los recursos son activos físico o de información que se evalúan en una auditoría. Algunos ejemplos de recursos de AWS son las instancias de Amazon EC2, las instancias de Amazon RDS, los buckets de Amazon S3 y subredes de Amazon VPC.

Evaluación de recursos

Las evaluaciones de recursos son los procesos mediante los cuales se evalúa un recurso, y se basan en requisitos de control. Mientras una evaluación está activa, Audit Manager evalúa cada

uno de los recursos que forman parte de la evaluación. Las evaluaciones de recursos ejecutan las tareas siguientes:

1. Recopilación de evidencias, incluidas las configuraciones de los recursos, los registros de eventos y los hallazgos
2. Traducción y asignación de las evidencias a los controles
3. Almacenamiento y rastreo del linaje de las evidencias para garantizar su integridad.

Conformidad de los recursos

El cumplimiento de los recursos se refiere al estado de evaluación de un recurso que se evaluó al recopilar las evidencias de verificación de cumplimiento.

Audit Manager recopila evidencias de verificación de conformidad para los controles que utilizan AWS Config y Security Hub como tipo de origen de datos. Es posible que se evalúen varios recursos durante la recopilación de evidencias. En consecuencia, una sola prueba de verificación de conformidad puede incluir uno o más recursos.

Utilice el filtro de cumplimiento de los recursos del buscador de evidencias para conocer el estado de cumplimiento a nivel de recursos. Una vez completada la búsqueda, puede obtener una vista previa de los recursos que coinciden con su consulta de búsqueda.

En el buscador de evidencias, hay tres valores posibles que determinan el cumplimiento de los recursos:

- No conforme: se refiere a los recursos con problemas de verificación de conformidad. Estos problemas se producen cuando Security Hub informa de un resultado de error para el recurso o de un resultado de AWS Config de no conformidad.
- Conforme: se refiere a los recursos que no tienen problemas de comprobaciones de conformidad. Esto sucede si Security Hub informa de un resultado de aprobado para el recurso o si de un resultado de AWS Config de conformidad.
- No concluyente: este filtro agrupa recursos para los cuales no hay una comprobación de conformidad disponible o aplicable. Esto ocurre si el tipo de origen de datos subyacente es AWS Config o Security Hub, pero esos servicios no están habilitados. También puede ocurrir si el tipo de origen de datos subyacente no admite comprobaciones de conformidad (como evidencias manuales, llamadas a la AWS API o CloudTrail).

S

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Servicio incluido

Se trata de Servicio de AWS incluidos en la evaluación. Cuando se especifica que un servicio se incluye en el alcance de la evaluación, Audit Manager evalúa los recursos de dicho servicio. Audit Manager puede evaluar una gran variedad de recursos de servicios como, por ejemplo los siguientes:

- Una instancia de Amazon EC2
- Un bucket de S3
- Usuario o rol
- Una tabla de DynamoDB
- Un componente de red, como una nube privada virtual (VPC) de Amazon, un grupo de seguridad o una lista de control de acceso (ACL).

Cuando se utiliza la consola Audit Manager para crear o actualizar una evaluación a partir de un marco estándar, la lista de Servicios de AWS incluida se selecciona de forma predeterminada. Esta lista no se puede editar Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. La selección se realiza de acuerdo con los requisitos del marco estándar. Si el marco estándar que ha seleccionado contiene solo controles manuales, no se incluirá ningún Servicios de AWS en su evaluación y no puede añadir ningún servicio a su evaluación.

Si necesita editar la lista de servicios incluidos en un marco estándar, puede hacerlo mediante las operaciones de la API de creación CreateAssessment o actualización UpdateAssessment. También puede personalizar el marco estándar y, a continuación, crear una evaluación a partir de dicho marco.

> **Note**
>
> Tenga en cuenta que el alcance de un servicio es diferente a un tipo de origen de datos, que también puede ser un tipo de origen de datos de Servicio de AWS o algo diferente. Para más información, consulte ¿Cuál es la diferencia entre un servicio incluido y un tipo de origen de datos? en el apartado de solución de problemas de esta guía.

¿Cómo recopila AWS Audit Manager las evidencias?

Cada evaluación activa en AWS Audit Manager recopila evidencias de varios orígenes de datos automáticamente, y tiene un ámbito definido que especifica los Servicios de AWS y cuentas de donde Audit Manager recopila los datos. Cada uno de estos servicios y cuentas definidos que se incluyen en el ámbito de aplicación contiene varios recursos, y cada recurso es un inventario de activos del sistema del cual usted es responsable. La recopilación de evidencias en Audit Manager implica evaluar cada uno de los recursos incluidos. Esto se conoce como evaluación de recursos.

Los siguientes pasos describen cómo Audit Manager recopila las evidencias para las evaluaciones de recursos:

1. Evaluar un recurso a partir del origen de datos

Para iniciar la recopilación de evidencias, Audit Manager evalúa los recursos internos a partir de un origen de datos. Para ello, captura una instantánea de la configuración, el resultado de una comprobación de conformidad relacionada y cualquier actividad de los usuarios. A continuación, ejecuta un análisis para determinar qué control admiten estos datos. Luego, se guarda el resultado de la evaluación de los recursos y se convierte en evidencia. Para más información sobre los diferentes tipos de evidencia, consulte Evidencias en el apartado de AWS Audit Managerconceptos y terminología de esta guía.

2. Pasos para convertir los resultados de la evaluación en evidencia

El resultado de las evaluaciones de un recurso contiene tanto los datos originales del recurso que se capturaron como los metadatos que indican qué control admiten los datos. AWS Audit Manager convierte los datos originales a un formato fácil de usar para los auditores. A continuación, los datos y metadatos convertidos se guardan como evidencia de Audit Manager antes de agregarlos a un control.

3. Cómo agregar evidencias al control correspondiente

Audit Manager lee los metadatos de las evidencias y agregas las evidencias guardadas a un control relacionado dentro de la evaluación. Las evidencias agregadas se hacen visibles en Audit Manager, y así se completa el ciclo de las evaluaciones de recursos.

> **Note**
>
> En algunos casos, se puede agregar la misma evidencia a varios controles de varias evaluaciones de Audit Manager según la configuración de control. Cuando se agrega la

misma evidencia a varios controles, Audit Manager mide la evaluación de los recursos exactamente una vez. Esto se debe a que la misma evidencia se recopila exactamente una sola vez. Sin embargo, un control de una evaluación de Audit Manager puede tener múltiples evidencias de múltiples orígenes de datos.

Frecuencia de recolección de evidencias

La recopilación de evidencias es un proceso continuo que comienza cuando se crea la evaluación. AWS Audit Manager recopila evidencias de varios orígenes de datos con diferentes frecuencias. Por lo tanto, la frecuencia con la que se recopilan las evidencias es cambiante: Depende del tipo y el origen de datos, como se describe a continuación.

- Comprobaciones de conformidad: Audit Manager recopila este tipo de evidencia de AWS Security Hub y AWS Config.
  - En el caso de AWS Security Hub, la frecuencia de la recopilación de evidencias sigue la planificación de las comprobaciones de Security Hub. Para más información sobre la programación de las comprobaciones de Security Hub, consulte Programación para la ejecución de las comprobaciones de seguridad en la AWS Security HubGuía del usuario. Para más información sobre las comprobaciones de Security Hub compatibles con Audit Manager, consulte AWS Security Hub controles compatibles con AWS Audit Manager.
  - Para AWS Config, la frecuencia de recopilación de evidencias sigue los desencadenantes definidos en las normas de AWS Config. Para más información sobre los desencadenadores de las reglas de AWS Config, consulte los tipos de desencadenadores en la Guía del usuario de AWS Config. Para más información sobre los elementos deReglas de AWS Config compatibles con Audit Manager, consulte Reglas de AWS Config con el apoyo de AWS Audit Manager.
- Actividad del usuario: Audit Manager recopila este tipo de evidencia de AWS CloudTrail de forma continua. En este caso la frecuencia es continua porque la actividad del usuario puede ocurrir en cualquier momento del día. Para más información, consulte AWS CloudTrail nombres de eventos compatibles con AWS Audit Manager.
- Configuración de datos: Audit Manager recopila este tipo de evidencia mediante una llamada de API de descripción a otra Servicio de AWS como Amazon EC2, Amazon S3 o IAM. Puede determinar las acciones de la API a las que desea llamar. También puede configurar la frecuencia como diaria, semanal o mensual en Audit Manager al crear o editar un control en la biblioteca de controles. Para obtener instrucciones sobre cómo crear y configurar un control, consulte Biblioteca

de control. Para más información sobre cómo Audit Manager utiliza las llamadas a la API para crear evidencias, consulte Las llamadas a la API son compatibles con AWS Audit Manager.

Independientemente de la frecuencia de recopilación de evidencias para el origen de datos, las nuevas evidencias se recopilarán automáticamente mientras el control y la evaluación estén activos.

Ejemplos de controles de AWS Audit Manager

Consulte los ejemplos de esta página para obtener más información sobre cómo funcionan los controles en AWS Audit Manager. Estos ejemplos muestran el aspecto de un control, cómo Audit Manager genera evidencias para ese control y los siguientes pasos que puede dar para demostrar conformidad.

> **Tip**
>
> Le recomendamos que habilite AWS Config y AWS Security Hub para disfrutar de una experiencia óptima en Audit Manager. Al habilitar estos servicios, podrá usarlos como un tipo de origen de datos para los controles de sus evaluaciones de Audit Manager. En otras palabras, Audit Manager puede utilizar los resultados de Security Hub y Reglas de AWS Config para generar evidencias automatizadas.
>
> - Una vez que AWS Security Hub estén habilitados, asegúrese de activar también todos los estándares de seguridad y de activar la configuración de los hallazgos de control consolidados. Así se asegurará de que Audit Manager pueda importar los resultados de todos los estándares de conformidad compatibles.
> - Una vez que estén habilitadosAWS Config, recuerde habilitar también Reglas de AWS Config relevantes o implementar un paquete de conformidad para la norma de conformidad relacionada con la auditoría. De este modo, Audit Manager podrá importar los resultados de todas las Reglas de AWS Config compatibles que haya habilitado.

Consulte los ejemplos disponibles para cada uno de los siguientes tipos de controles a continuación:

Temas

- Controles automatizados que utilizan AWS Security Hub como tipo de origen de datos
- Controles automatizados que utilizan AWS Config como tipo de origen de datos
- Controles automatizados que utilizan las llamadas a la AWS API como tipo de origen de datos

- Controles automatizados que utilizan AWS CloudTrail como tipo de origen de datos
- Controles manuales
- Controles con distintos tipos de orígenes de datos (automatizados y manuales)

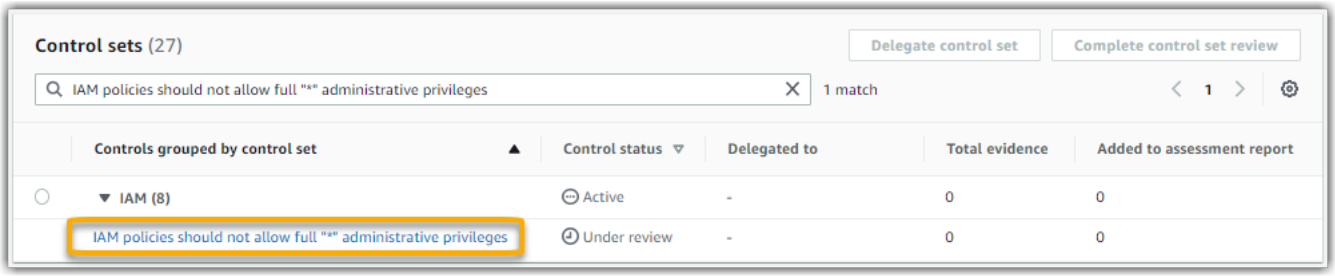
Controles automatizados que utilizan AWS Security Hub como tipo de origen de datos

En este ejemplo se muestra un control que utiliza AWS Security Hub como tipo de origen de datos. Se trata de un control estándar tomado del marco de AWSprácticas recomendadas de seguridad fundamentales (FSBP). Audit Manager utiliza este control para generar evidencias que pueden ayudarle a alinear su entorno de AWS con los requisitos del FSBP.

Ejemplo de detalles de control

- Nombre del control: `IAM policies should not allow full "*" administrative privileges`
- Conjunto de controles: este control pertenece al conjunto de controles de `IAM`. Se trata de un grupo de controles relacionados con la administración de identidades y accesos.
- Tipo de origen de datos: AWS Security Hub
- Tipo de evidencia: comprobaciones de conformidad

En el siguiente ejemplo, este control se encuentra dentro de una evaluación de Audit Manager que se creó a partir del marco FSBP.



La evaluación muestra el estado del control, También muestra el número de evidencias recopiladas para el control hasta el momento y cuántas de ellas se incluyen en el informe de evaluación. A partir de este punto puede delegar la revisión del conjunto de controles o completar la revisión por su cuenta. Al elegir el nombre del control se abrirá una página de detalles con más información, incluidas las evidencias del control.

Cómo funciona el control

Audit Manager puede utilizar este control para comprobar si sus políticas de IAM son demasiado amplias para cumplir los requisitos del FSBP. Más específicamente, puede comprobar si las políticas de IAM administradas por sus clientes tienen acceso de administrador, lo que incluye la siguiente declaración comodín: `"Effect": "Allow"` con `"Action": "*"` de más de `"Resource": "*"`

Cómo recopila Audit Manager las evidencias para el control

Audit Manager sigue los pasos que se detallan a continuación para recopilar evidencias para el control:

1. Para cada control, Audit Manager evalúa los recursos incluidos. Para ello, utiliza el origen de datos que se especifica en la configuración del control. En este ejemplo, las políticas de IAM son el recurso y Security Hub AWS Config son el tipo de origen de datos. Audit Manager busca el resultado de una comprobación específica de Security Hub ([IAM.1]), que a su vez utiliza una AWS Config regla para evaluar las políticas de IAM (iam-policy-no-statements-with-admin-access).
2. El resultado de la evaluación de los recursos se guarda y se convierte en evidencias de fácil acceso para el auditor. Audit Manager genera evidencias de verificación de conformidad para los controles que utilizan Security Hub como tipo de origen de datos. Esta evidencia contiene el resultado de las comprobaciones de conformidad notificado directamente desde Security Hub.
3. Audit Manager agrega las evidencias guardadas al control de la evaluación denominado “`IAM policies should not allow full "*" administrative privileges`”.

Cómo puede utilizar Audit Manager para demostrar la conformidad del control

Una vez agregadas las evidencias al control, usted (o un delegado de su elección) puede revisarlas para ver si es necesaria alguna corrección.

En este ejemplo, Audit Manager puede mostrar una regla de error de Security Hub. Esto puede suceder si sus políticas de IAM contienen caracteres comodín (*) y son demasiado amplias para poder controlarlas. En este caso, puede actualizar sus políticas de IAM para que no permitan todos los privilegios de administrador. Determine las tareas que tienen que realizar los usuarios y elabore políticas al respecto para permitirles realizar solo esas tareas. Esta acción correctiva ayuda a alinear su AWS entorno con los requisitos de FSBP.

Cuando sus políticas de IAM estén en línea con el control, marque el control como revisado y añada las evidencias a su informe de evaluación. A continuación puede compartir este informe con los auditores para mostrar que el control funciona según lo previsto.

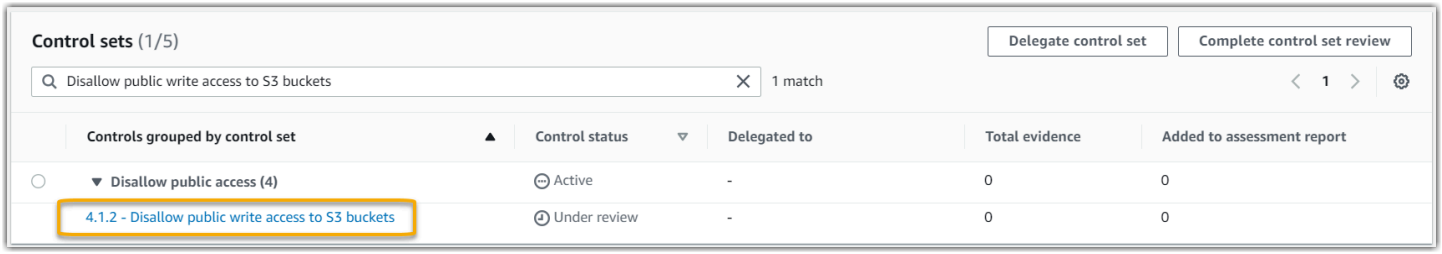
Controles automatizados que utilizan AWS Config como tipo de origen de datos

En este ejemplo se muestra un control que utiliza AWS Config como tipo de origen de datos. Se trata de un control estándar tomado del AWS Control Towermarco de barreras de protección. Audit Manager utiliza este control para generar evidencias que pueden ayudar a alinear su AWS entorno con las AWS Control Tower barreras de protección.

Ejemplo de detalles de control

- Nombre del control: `4.1.2 - Disallow public write access to S3 buckets`
- Conjunto de controles: este control pertenece al conjunto de controles de `Disallow public access`. Se trata de una agrupación de controles relacionados con la administración de accesos.
- Tipo de origen de datos: AWS Config
- Tipo de evidencia: comprobaciones de conformidad

En el siguiente ejemplo, el control se encuentra dentro de una evaluación de Audit Manager que se creó a partir del AWS Control Towermarco de barreras de protección.



También muestra el estado de control, cuántas evidencias recopiladas se recopilaron para este control hasta el momento y cuántas de ellas se incluyen en el informe de evaluación. A partir de este punto puede delegar la revisión del conjunto de controles o completar la revisión por su cuenta. Al elegir el nombre del control se abrirá una página de detalles con más información, incluidas las evidencias del control.

Cómo funciona el control

Audit Manager puede usar este control para comprobar si los niveles de acceso de sus políticas de bucket de S3 son demasiado flexibles para cumplir con los requisitos de AWS Control Tower. En concreto, puede comprobar la configuración de bloqueo de acceso público, las políticas de los buckets y las listas de control de acceso (ACL) a los buckets para confirmar que los buckets no permiten el acceso público de escritura.

Cómo recopila Audit Manager las evidencias para el control

Audit Manager sigue los pasos que se detallan a continuación para recopilar evidencias para el control:

1. Para cada control, Audit Manager evalúa los recursos incluidos en el ámbito utilizando el origen de datos que se especifica en la configuración del control. En este caso, los depósitos de S3 son el recurso y, AWS Config, el tipo de origen de datos. Audit Manager busca el resultado de una regla de AWS Config específica (s3-bucket-public-write-prohibited) para evaluar la configuración, la política y la ACL de cada uno de los grupos de S3 que se deben evaluar.
2. El resultado de la evaluación de los recursos se guarda y se convierte en evidencias de fácil acceso para el auditor. Audit Manager genera evidencias de verificación de conformidad para los controles que se AWS Config utilizan como tipo de origen de datos. Esta evidencia contiene el resultado de la comprobación de conformidad informado directamente desde AWS Config.
3. Audit Manager agrega las evidencias guardadas al control de la evaluación denominado "`4.1.2 - Disallow public write access to S3 buckets`".

Cómo puede utilizar Audit Manager para demostrar la conformidad del control

Una vez agregadas las evidencias al control, usted (o un delegado de su elección) puede revisarlas para ver si es necesaria alguna corrección.

En este ejemplo, Audit Manager puede mostrar una regla de AWS Config que indica que un resultado de no conformidad para un bucket de S3. Esto puede ocurrir si uno de sus buckets de S3 tiene una configuración de bloqueo de acceso público que no restringe las políticas públicas y la política que está en uso permite el acceso de escritura público. Para remediarlo, puede actualizar la configuración Bloquear el acceso público para restringir las políticas públicas. Otra opción es usar una política de bucket diferente que no permita el acceso de escritura público. Esta acción correctiva le ayudará a ajustar su entorno de AWS de acuerdo con los requisitos de AWS Control Tower.

Compruebe que los niveles de acceso al bucket de S3 concuerdan con los del control, marque el control como revisado y añada las evidencias a su informe de evaluación. A continuación puede compartir este informe con los auditores para mostrar que el control funciona según lo previsto.

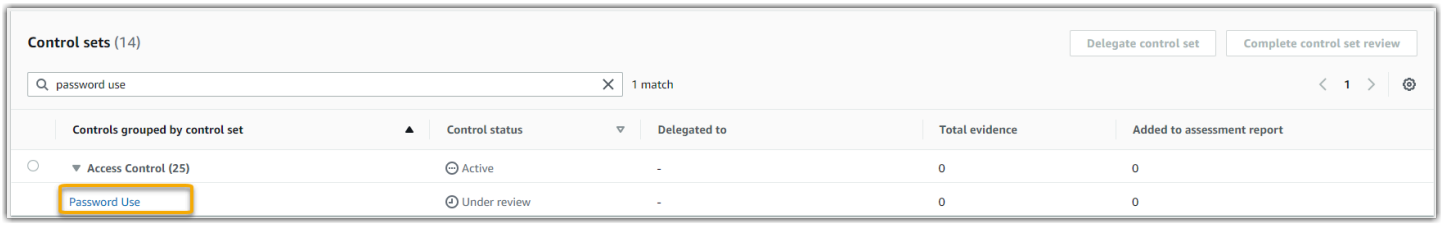
Controles automatizados que utilizan las llamadas a la AWS API como tipo de origen de datos

En este ejemplo se muestra un control personalizado que utiliza llamadas a la AWS API como tipo de origen de datos. Audit Manager lo utiliza para generar evidencias que pueden ayudar a adaptar su entorno de AWS a sus requisitos específicos.

Ejemplo de detalles de control

- Nombre del control: `Password Use`
- Conjunto de controles: este control pertenece a un conjunto de controles denominado "`Access Control`". Se trata de un grupo de controles relacionados con la administración de identidades y accesos.
- Tipo de origen de datos: llamadas a la API de AWS
- Tipo de evidencia: datos de configuración

En el siguiente ejemplo este control se encuentra dentro de una evaluación de Audit Manager creada a partir de un marco personalizado.



La evaluación muestra el estado del control, También muestra el número de evidencias recopiladas para el control hasta el momento y cuántas de ellas se incluyen en el informe de evaluación. A partir de este punto puede delegar la revisión del conjunto de controles o completar la revisión por su cuenta. Al elegir el nombre del control se abrirá una página de detalles con más información, incluidas las evidencias del control.

Cómo funciona el control

Audit Manager puede utilizar este control personalizado para ayudarle a garantizar que cuenta con políticas de control de acceso suficientes. Este control requiere que siga las buenas prácticas de seguridad en la selección y el uso de las contraseñas. Audit Manager puede resultar útil a la hora de obtener una lista de todas las políticas de contraseñas de los directores de IAM que se incluyen en su evaluación.

Cómo recopila Audit Manager las evidencias para el control

Audit Manager sigue los pasos que se detallan a continuación para recopilar evidencias para los controles personalizados.

1. Para cada control, Audit Manager evalúa los recursos incluidos en el ámbito utilizando el origen de datos que se especifica en la configuración del control. En este caso, los IAM principales son los recursos y las llamadas a la API de AWS son el tipo de origen de datos. Audit Manager busca el resultado de una llamada a la API de IAM (GetAccountPasswordPolicy) específica. A continuación, devuelve las políticas de contraseñas de Cuentas de AWS que se evalúan.
2. El resultado de la evaluación de los recursos se guarda y se convierte en evidencias de fácil acceso para el auditor. Audit Manager genera evidencias de datos de configuración para los controles que utilizan llamadas a la API como origen de datos. Esta evidencia contiene los datos originales que se capturan de las respuestas de la API y metadatos adicionales que indican qué control admiten los datos.
3. Audit Manager agrega la evidencia o evidencias guardadas al control personalizado de la evaluación que se denomina "`Password Use`".

Cómo puede utilizar Audit Manager para demostrar la conformidad del control

Una vez agregadas las evidencias al control, usted (o un delegado de su elección) podrá revisarlas para comprobar si son suficientes o si es necesario corregirlas.

Revise las evidencias de este ejemplo para ver las respuestas de la llamada a la API. La respuesta de GetAccountPasswordPolicy describe los requisitos de complejidad y los períodos de rotación obligatorios para las contraseñas de usuarios de su cuenta. Puede utilizar esta respuesta de la API como prueba para demostrar que cuenta con políticas de control de acceso mediante contraseñas suficientes para Cuentas de AWS que son objeto de evaluación. Si lo desea, también puede hacer comentarios adicionales sobre estas políticas añadiendo anotaciones al control.

Compruebe que las políticas de contraseñas de sus directores de IAM se ajustan al control personalizado, marque el control como revisado y añada las evidencias a su informe de evaluación. A continuación puede compartir este informe con los auditores para mostrar que el control funciona según lo previsto.

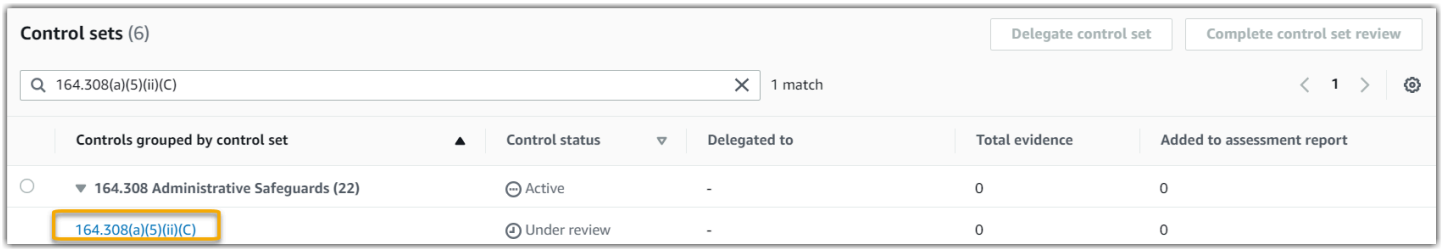
Controles automatizados que utilizan AWS CloudTrail como tipo de origen de datos

En este ejemplo se muestra un control que utiliza AWS CloudTrail como tipo de origen de datos. Se trata de un control estándar tomado del marco de la HIPAA. Audit Manager lo utiliza para generar evidencias que pueden serle de utilidad para hacer que su entorno de AWS corresponda con los requisitos de la HIPAA.

Ejemplo de detalles de control

- Nombre del control: `164.308(a)(5)(ii)(C)`
- Conjunto de controles: este control pertenece al conjunto de controles denominado "`164.308 Administrative Safeguards`".
- Tipo de origen de datos: AWS CloudTrail
- Tipo de evidencia: actividad del usuario

Este control se muestra en una evaluación de Audit Manager creada a partir del marco de la HIPAA:



La evaluación muestra el estado del control, También muestra el número de evidencias recopiladas para el control hasta el momento y cuántas de ellas se incluyen en el informe de evaluación. A partir de este punto puede delegar la revisión del conjunto de controles o completar la revisión por su cuenta. Al elegir el nombre del control se abrirá una página de detalles con más información, incluidas las evidencias del control.

Cómo funciona el control

Este control requiere un procedimiento de supervisión para detectar inicios de sesión inadecuados. Los inicios de sesión inapropiados se producen, por ejemplo, cuando se introducen varias combinaciones de nombres de usuario o contraseñas para intentar acceder a un sistema de información. Audit Manager le ayuda a validar este control proporcionándole una lista de todos los intentos de inicio de sesión detectados para los recursos que evalúa.

Cómo recopila Audit Manager las evidencias para el control

Audit Manager sigue los pasos que se detallan a continuación para recopilar evidencias para el control:

1. Para cada control, Audit Manager evalúa los recursos incluidos en el ámbito utilizando el origen de datos que se especifica en la configuración del control. En este caso, los usuarios son el recurso y CloudTrail es el tipo de origen de datos. Audit Manager busca el resultado de todos los eventos de inicio de sesión de la consola de administración de AWS que CloudTrail registra. A continuación, devuelve un registro de los eventos relevantes detectados como resultado de la evaluación.
2. El resultado de la evaluación de los recursos se guarda y se convierte en evidencias de fácil acceso para el auditor. Audit Manager genera evidencias de la actividad de los usuarios para los controles que utilizan CloudTrail como tipo de origen de datos. Esta evidencia contiene los datos originales de los usuarios que se detectan y metadatos adicionales que indican qué control admiten los datos.
3. Audit Manager agrega las evidencias guardadas al control de la evaluación denominado "`164.308(a)(5)(ii)(C)`".

Cómo puede utilizar Audit Manager para demostrar la conformidad del control

Una vez agregadas las evidencias al control, usted (o un delegado de su elección) puede revisarlas para ver si es necesaria alguna corrección.

En este ejemplo, puede revisar las evidencias para ver los eventos de inicio de sesión que ha registrado CloudTrail. Este registro describe la actividad de inicio de sesión de sus usuarios en la consola e incluye la siguiente información:

- Todos los inicios de sesión exitosos
- Todos los intentos de inicio de sesión fallidos
- La verificación de cuándo se aplicó la autenticación multifactor (MFA)
- La dirección IP de todos los inicios de sesión

Puede utilizar este registro como prueba para demostrar que cuenta con suficientes procedimientos de supervisión para las Cuentas de AWS que sean objeto de evaluación. Si lo desea, también puede aportar comentarios adicionales agregando comentarios al control. Por ejemplo, si el registro muestra alguna discrepancia, como varios intentos de inicio de sesión fallidos, puede añadir una anotación que explique cómo solucionó el problema. La supervisión periódica de los inicios de

sesión en la consola le será de utilidad para evitar problemas de seguridad que puedan derivarse de las discrepancias y de los intentos de inicio de sesión inadecuados. A su vez, esta práctica recomendada ayuda a adaptar su entorno de AWS a los requisitos de la HIPAA.

Cuando compruebe que su procedimiento de monitoreo está en consonancia con el control puede marcar el control como revisado y agregar las evidencias al informe de evaluación. A continuación puede compartir este informe con los auditores para mostrar que el control funciona según lo previsto.

Controles manuales

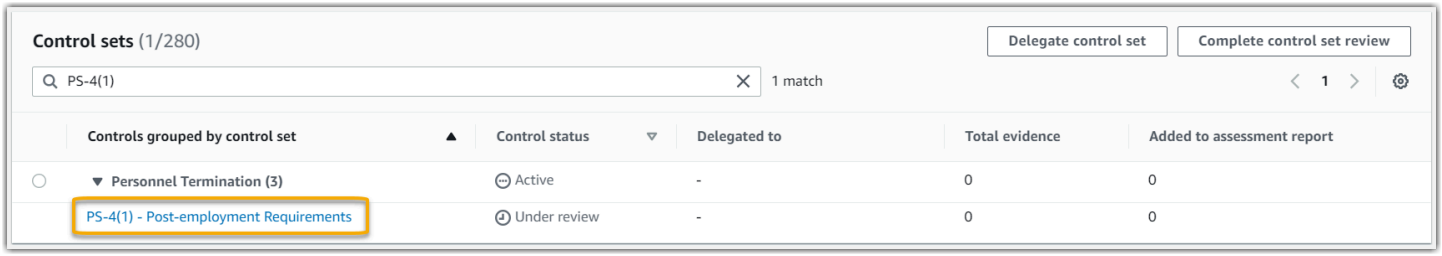
Algunos controles no admiten la recopilación automática de evidencia. Esto incluye controles basados en el suministro de registros y firmas físicas, además de observaciones, entrevistas y otros eventos que no se generan en la nube. En estos casos puede cargar evidencias manualmente para demostrar que cumple con los requisitos del control.

Este ejemplo muestra un control manual para el cual Audit Manager no recopila evidencias automatizadas. Se trata de un control estándar tomado del marco NIST 800-53 (Rev. 5). Puede utilizar Audit Manager para cargar y almacenar evidencias que demuestren la conformidad del control.

Ejemplo de detalles de control

- Nombre del control: `PS-4(1) - Post-employment Requirements`
- Conjunto de controles: este control pertenece al conjunto de controles de `Personnel Termination`. Se trata de una serie de controles relacionados con la seguridad de la información en el contexto de los procedimientos de despido.
- Tipo de origen de datos: manual
- Tipo de evidencia: manual

Este control se muestra en una evaluación de Audit Manager creada a partir del marco NIST 800-53 (Rev. 5) Bajo-Moderado-Alto.



La evaluación muestra el estado del control, También muestra el número de evidencias recopiladas para el control hasta el momento y cuántas de ellas se incluyen en el informe de evaluación. A partir de este punto puede delegar la revisión del conjunto de controles o completar la revisión por su cuenta. Al elegir el nombre del control se abrirá una página de detalles con más información, incluidas las evidencias del control.

Cómo funciona el control

Puede usar este control para confirmar que está protegiendo la información de la organización en caso de despido de un empleado. En concreto, puede demostrar que informa sistemáticamente a las personas despedidas de los requisitos aplicables y legalmente vinculantes posteriores a la contratación relativa a la protección de la información de la organización o empresa. Además, puede demostrar que todas las personas despedidas firman un acuse de recibo de los requisitos posteriores a la contratación como parte del proceso de despido en su organización o empresa.

¿Cómo puedo cargar las evidencias de este control manualmente?

Siga los pasos que se detallan a continuación para cargar evidencias manuales de acuerdo con este control:

1. Coloque la evidencia manual que dese cargar en un bucket de Amazon Simple Storage Service (S3) y anote el URI de S3.
2. En la evaluación de Audit Manager, abra el control, vaya a la pestaña de carpetas de evidencias y cargue las evidencias introduciendo el URI de S3. Para más información, consulte Carga manual de evidencias en AWS Audit Manager.
3. Audit Manager crea una carpeta de evidencias que lleva el nombre de la fecha en que se cargaron las evidencias. Audit Manager agrega las evidencias subidas al control de la evaluación denominado “`PS-4(1) - Post-employment Requirements`”.

Cómo puede utilizar Audit Manager para demostrar la conformidad del control

Si tiene documentación que respalde este control, puede cargarla como evidencia manual. Por ejemplo, puede subir la última copia de los requisitos post-empleo legalmente vinculantes que su departamento de Recursos Humanos expide a los empleados despedidos. Si se despidió a alguna persona durante el período de auditoría, también puede subir copias fechadas dirigidas a esas personas despedidas.

Al igual que con los controles automatizados, puede delegar los controles manuales en las partes interesadas, quienes pueden ayudarle a revisar las evidencias (o, en este caso, a proporcionarlas).

Por ejemplo, al revisar este control, es posible que se dé cuenta de que solo cumple parcialmente sus requisitos. Este podría ser el caso si no tiene una carta de reconocimiento firmada por una persona despedida. Puedes delegar el control en una parte interesada de Recursos Humanos, quien luego podrá subir una copia de la carta firmada. O bien, si no se despidió a ningún empleado durante el período de auditoría, puede dejar un comentario en el que se explique por qué no se agregan cartas firmadas al control.

Cuando confirme que está de acuerdo con el control, puede marcarlo como revisado y añadir las evidencias al informe de evaluación. A continuación puede compartir este informe con los auditores para mostrar que el control funciona según lo previsto.

Controles con distintos tipos de orígenes de datos (automatizados y manuales)

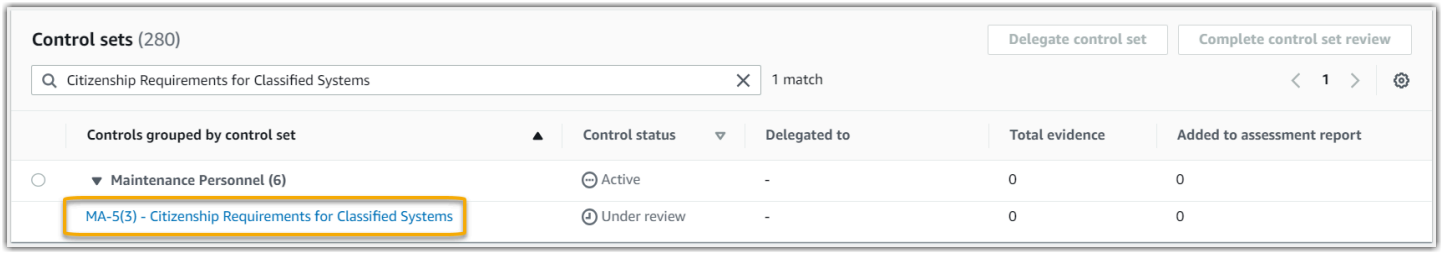
En muchos casos, se necesita una combinación de evidencias automatizadas y manuales para cumplir con un control. Si bien Audit Manager puede proporcionar evidencias automatizadas que sean relevantes para el control, es posible que deba complementar estos datos con evidencias manuales que identifique y cargará manualmente

En este ejemplo, se muestra un control que utiliza una combinación de evidencia manuales y evidencias automatizadas que provienen de las llamadas a la AWS API. Se trata de un control estándar tomado del marco NIST 800-53 (Rev. 5). Audit Manager utiliza este control para generar evidencias que pueden ayudar a adaptar su AWS entorno de acuerdo con los requisitos del NIST.

Ejemplo de detalles de control

- Nombre del control: `MA-5(3) - Citizenship Requirements for Classified Systems`
- Conjunto de controles: este control pertenece al conjunto de controles de `Maintenance Personnel`. Se trata de una agrupación de controles que se refiere a las personas que realizan el mantenimiento del hardware o el software de los sistemas de la organización.
- Tipo de origen de datos: llamadas a la AWS API, más evidencias manuales complementarias
- Tipo de evidencia: datos de configuración

Este es el control que se muestra en una evaluación de Audit Manager que se creó a partir del marco NIST 800-53 (Rev. 5):



La evaluación muestra el estado del control, También muestra el número de evidencias recopiladas para el control hasta el momento y cuántas de ellas se incluyen en el informe de evaluación. A partir de este punto puede delegar la revisión del conjunto de controles o completar la revisión por su cuenta. Al elegir el nombre del control se abrirá una página de detalles con más información, incluidas las evidencias del control.

Cómo funciona el control

Audit Manager puede usar este control para ayudarlo a garantizar que el personal que realiza sus actividades de mantenimiento y diagnóstico tenga el estado de ciudadanía requerido. Si su sistema procesa, almacena o transmite información clasificada, debe demostrar que el personal de mantenimiento es ciudadano estadounidense. Audit Manager le ayuda a validarlo. Para ello, devuelve una lista completa de todas las políticas y principios de la IAM que forman parte de su evaluación. A continuación, podrá comprobar y demostrar que esta lista de usuarios cumple los requisitos de ciudadanía necesarios. Para ello, puede cargar manualmente evidencias adicionales de su estado de ciudadanía.

Cómo recopila Audit Manager las evidencias para el control

Audit Manager sigue los pasos que se detallan a continuación para recopilar evidencias para el control:

1. Para cada control, Audit Manager evalúa los recursos incluidos en el ámbito utilizando el origen de datos que se especifica en la configuración del control. En este caso, sus políticas y principios de IAM son los recursos y las llamadas a la AWS API son el origen de datos. Audit Manager busca el resultado de cuatro llamadas específicas a la API de IAM (ListUsers/ListRoles/ListGroups/ListPolicies) y devuelve una lista de las políticas y principios de IAM que forman parte de su evaluación.
2. El resultado de la evaluación de los recursos se guarda y se convierte en evidencias de fácil acceso para el auditor. Audit Manager genera evidencias de datos de configuración para los controles que utilizan llamadas a la API como tipo de origen de datos. Esta evidencia contiene los

datos originales que se capturan de las respuestas de la API y metadatos adicionales que indican qué control admiten los datos.

3. Audit Manager agrega las evidencias guardadas al control de la evaluación denominado "`MA-5(3) - Citizenship Requirements for Classified Systems`".

¿Cómo puedo cargar las evidencias de este control manualmente?

Siga los pasos que se detallan a continuación para cargar evidencias manuales que complementen las automatizadas:

1. Coloque la documentación de ciudadanía en un bucket de Amazon Simple Storage Service (Amazon S3) y anote el URI de S3.
2. En su evaluación de Audit Manager, abra el control, vaya a la pestaña de carpetas de evidencias y cargue las evidencias. Para ello, introduzca el URI de S3. Para obtener instrucciones, consulte Agregar evidencias manuales AWS Audit Manager.
3. Audit Manager agrega la evidencia cargada al control de la evaluación llamada "`MA-5(3) - Citizenship Requirements for Classified Systems`".

Cómo puede utilizar Audit Manager para demostrar la conformidad del control

Una vez agregadas las evidencias al control, usted (o un delegado de su elección) podrá revisarlas para comprobar si son suficientes o si es necesario corregirlas.

El ejemplo siguiente muestra las evidencias y una lista de 20 usuarios. Si tiene dudas sobre cómo identificar qué usuarios son personal de mantenimiento o de qué ciudadanía tienen esos usuarios, puede delegar el control en un experto en la materia para que lo valide. El delegado puede confirmar la lista del personal de mantenimiento y cargar manualmente las evidencias adicionales como documentación de su estado de ciudadanía. Confirmar la ciudadanía de todos los usuarios relevantes de la lista ayuda a adaptar su entorno de AWS a los requisitos del NIST. Si su sistema no procesa, almacena ni transmite información clasificada, puede dejar un comentario en el que se explique por qué no se aplica este control.

Confirme que está de acuerdo con el control, márquelo como revisado y añada las evidencias al informe de evaluación. A continuación puede compartir este informe con los auditores para mostrar que el control funciona según lo previsto.

Integraciones con Servicios de AWS relacionados

AWS Audit Manager se integra con varios Servicios de AWS para recopilar evidencias automáticamente que puede incluir en sus informes de evaluación.

AWS Security Hub

AWS Security Hub supervisa su entorno mediante comprobaciones de seguridad automatizadas que se basan en las mejores prácticas y los estándares de AWS. Audit Manager captura instantáneas del estado de seguridad de sus recursos informando de los resultados de las comprobaciones de seguridad directamente desde Security Hub. Para más información acerca de Security Hub, consulte ¿Qué es AWS Security Hub? en la Guía del usuario de AWS Security Hub.

AWS CloudTrail

AWS CloudTrail le ayuda a supervisar las llamadas realizadas a los recursos de AWS de su cuenta. Esto incluye las llamadas realizadas por la consola de administración de AWS, la CLI de AWS y otros Servicios de AWS. Audit Manager recopila los datos de registro directamente de CloudTrail y convierte los registros procesados en evidencias de la actividad del usuario. Para más información acerca de CloudTrail, consulte ¿Qué es AWS CloudTrail? en la Guía del usuario de AWS CloudTrail.

AWS Config

AWS Config proporciona una vista detallada de la configuración de los recursos de AWS de su Cuenta de AWS. Esto incluye cómo se relacionan los recursos entre sí y cómo se configuraron anteriormente. Audit Manager captura una instantánea del estado de seguridad de sus recursos mediante un informe de los resultados obtenidos de AWS Config. Para más información sobre AWS Config, consulte ¿Qué es AWS Config? en la Guía del usuario de AWS Config.

AWS License Manager

AWS License Manager simplifica el proceso de llevar licencias de proveedores de software a la nube. A medida que cree la infraestructura de nube de AWS, puede ahorrar en costos reconvirtiendo su inventario de licencias para utilizarlo con los recursos de la nube. Audit Manager incluye un marco de License Manager para ayudarlo en la preparación de la auditoría. Este marco se integra con License Manager para agregar información sobre el uso de licencias en función de las reglas de concesión de licencias definidas por el cliente. Para más información acerca de License Manager, consulte ¿Qué es AWS License Manager? en la Guía del usuario de AWS License Manager.

AWS Control Tower

AWS Control Tower impone barreras preventivas y medidas de seguridad de detección para la infraestructura de nube. Audit Manager proporciona un marco de AWS Control Tower de barreras de protección para ayudarlo en la preparación de la auditoría. Este marco contiene todas las normas de AWS Config basadas en las barreras de protección de AWS Control Tower. Para obtener más información sobre AWS Control Tower, consulte ¿Qué es AWS Control Tower? en la Guía del usuario de AWS Control Tower.

AWS Artifact

AWS Artifact es un portal de recuperación de artefactos de auditoría de autoservicio que proporciona acceso bajo demanda a la documentación de conformidad y las certificaciones de la infraestructura de AWS. AWS Artifact ofrece evidencias que demuestran que la infraestructura de la nube de AWS cumple los requisitos de conformidad. A su vez, le AWS Audit Manager ayuda a recopilar, revisar y gestionar evidencias para demostrar que usa los Servicios de AWS de acuerdo con con la normativa aplicable. Para más información sobre AWS Artifact, consulte ¿Qué es AWS Artifact? en la Guía del usuario de AWS Artifact. Puede descargar una lista de informes de AWS en la AWS Management Console.

Para obtener una lista de los Servicios de AWS incluidos en determinados programas de conformidad, consulte los Servicios de AWS incluidos en los programas de conformidad. Para más información general, consulte Programas de conformidad de AWS.

Integraciones con productos de terceros de GRC

AWS Audit Manager admite integraciones con los productos GRC de socios externos que se detallan en esta página.

Si su empresa utiliza un modelo de nube híbrida o multinube, es probable que utilice un producto GRC para gestionar las evidencias de esos entornos. Si se integra con Audit Manager, podrá obtener evidencias sobre su uso de AWS directamente en su entorno de GRC. Esto simplifica la gestión del cumplimiento ya que le proporciona un lugar centralizado para revisar y corregir las evidencias al prepararse para las auditorías.

En esta página se describen los productos GRC de terceros que pueden capturar evidencias de Audit Manager. También encontrará una referencia de las acciones de la API de Audit Manager que puede realizar directamente en esos productos.

Temas

Cómo funcionan las integraciones de terceros con Audit Manager

Los socios de GRC pueden usar las API públicas de Audit Manager para integrar sus productos con Audit Manager. Con esta integración, puede asignar los controles empresariales de su entorno de GRC a los controles de Audit Manager.

Solo tendrá que asignar el control una vez. Después de ello podrá crear las evaluaciones de Audit Manager directamente en el producto GRC. Esta acción inicia la recopilación de evidencias sobre el uso de AWS. A continuación, podrá ver estas evidencias de AWS junto con las demás evidencias recopiladas en su entorno híbrido, todo ello en el contexto de los controles de su empresa.

Tenga en cuenta los siguientes aspectos cuando utilice una integración de Audit Manager con un producto GRC de terceros:

- Las integraciones están disponibles para todas las Regiones de AWS donde se admite Audit Manager.
- Todos los recursos de Audit Manager que cree en el producto asociado de GRC también se reflejarán en Audit Manager.
- El uso está sujeto a los precios de AWS Audit Manager y del producto de GRC de terceros.
- Las evidencias que recopila Audit Manager son inmutables. Las evidencias se presentan exactamente de la misma manera en los productos GRC de terceros que en la consola Audit Manager. Sin embargo, si utiliza una integración de terceros, es posible que pueda mejorarlas agregando un contexto adicional en sus informes.
- Se aplican las mismas cuotas de Audit Manager al producto GRC de terceros. Por ejemplo, cada Cuenta de AWS puede tener hasta 100 evaluaciones de Audit Manager activas. Esta cuota a nivel de cuenta se aplica tanto si crea las evaluaciones en la consola Audit Manager como en el producto GRC de terceros. La mayoría de las cuotas de Audit Manager, aunque no todas, se enumeran en el espacio de nombres de AWS Audit Manager en la consola de Service Quotas. Para más información acerca de los aumentos de cuota, consulte Administrar las cuotas de Audit Manager.

Si tiene una solución de cumplimiento y desea integrarla con Audit Manager, envíe un correo electrónico a `auditmanager-partners@amazon.com`.

Productos de socios GRC de terceros que se integran con Audit Manager

Los siguientes productos de GRC de terceros pueden capturar evidencias de Audit Manager.

MetricStream

Si desea usar esta integración, póngase en contacto con MetricStream para acceder y comprar el software MetricStream GRC.

Basada en la plataforma MetricStream, la solución GRC empresarial de MetricStream ofrece un enfoque integral y colaborativo de las actividades y los procesos de GRC en toda la empresa. Al incorporar las evidencias de Audit Manager a MetricStream, puede identificar de forma proactiva las evidencias de su entorno de AWS que no cumplen con las normas y revisarlas junto con las de sus fuentes de datos locales o de otros socios de nube. Se trata de una forma cómoda y centralizada de revisar y mejorar su postura en materia de cumplimiento y seguridad en la nube al tiempo que se prepara para las auditorías.

Con la integración de MetricStream y Audit Manager, puede realizar las siguientes operaciones de API.

Tarea	Operación de la API
Configuración de la integración de Audit Manager	• GetAccountStatus • GetOrganizationAdminAccount • GetSettings
Revisión de los recursos de Audit Manager	• GetAssessment • GetAssessmentFramework • GetControl • ListAssessmentFrameworks • ListControls
Creación de recursos de Audit Manager	• CreateAssessment • CreateAssessmentFramework
Actualización de los recursos de Audit Manager	• UpdateAssessment • UpdateAssessmentControl

Tarea	Operación de la API
	• UpdateAssessmentStatus
Gestión de la evidencia	• StartQuery (API de AWS CloudTrail) • GetQueryResults (API AWS CloudTrail)
Eliminar recursos de Audit Manager	• DeleteAssessmentFramework

Enlaces relacionados con MetricStream

- AWS Marketplace.link
- Enlace al producto
- Precios del producto

Uso de Audit Manager con el SDK de AWS

Los kits de desarrollo de software (SDK) de AWS están disponibles en muchos lenguajes de programación populares. Cada SDK proporciona una API, códigos de ejemplo y documentación que los desarrolladores puede usar para crear aplicaciones en el lenguaje que prefieran.

Documentación de SDK	Documentación específica de Audit Manager	Ejemplos de código	
AWS SDK for C++	Referencia de API de AWS SDK for C++ para Audit Manager	Ejemplos de código de AWS SDK for C++	
AWS SDK for Go	Referencia de API de AWS SDK for Go para Audit Manager	Ejemplos de código de AWS SDK for Go	
AWS SDK for Java	Referencia de API de AWS SDK for Java 2.x para Audit Manager	Ejemplos de código de AWS SDK for Java	
AWS SDK for JavaScript	Referencia de API de AWS SDK for JavaScript para Audit Manager	Ejemplos de código de AWS SDK for JavaScript	

Documentación de SDK	Documentación específica de Audit Manager	Ejemplos de código	
AWS SDK for .NET	Referencia de API de AWS SDK for .NET para Audit Manager	Ejemplos de código de AWS SDK for .NET	
AWS SDK for PHP	Referencia de API de AWS SDK for PHP para Audit Manager	Ejemplos de código de AWS SDK for PHP	
AWS SDK for Python (Boto3)	Referencia de API de AWS SDK for Python (Boto) para Audit Manager	Ejemplos de código de AWS SDK for Python (Boto3)	
AWS SDK for Ruby	Referencia de API de AWS SDK for Ruby para Audit Manager	Ejemplos de código de AWS SDK for Ruby	

Para ver ejemplos específicos de Audit Manager, consulte Ejemplos de código para AWS Audit Manager.

> **Note**
>
> Audit Manager está disponible en la versión 1.19.32 de botocore y posteriores para AWS SDK for Python (Boto3). Antes de empezar a usar el SDK, asegúrese de que usa la versión botocore adecuada.

Configuración de AWS Audit Manager

Antes de empezar a utilizar Audit Manager, asegúrese de haber completado las siguientes tareas de configuración.

Temas

- Requisitos previos: crear una Cuenta de AWS y configurar los permisos
- Habilitar Audit Manager: utilice la consola, la AWS CLI o la API para habilitar Audit Manager
- Recomendaciones: Configure las integraciones recomendadas con otros Servicios de AWS

Requisitos previos

Siga estos pasos para crear una Cuenta de AWS y un usuario administrativo con privilegios de configuración de Audit Manager.

Pasos

- Registro para obtener una Cuenta de AWS
- Crear un usuario administrativo
- Añada los permisos mínimos necesarios para acceder a Audit Manager y habilitarlo

> **Important**
>
> Si ya ha configurado AWS e IAM, puede omitir los pasos 1 y 2. Sin embargo, debe realizar el paso 3 para asegurarse de que dispone de los permisos necesarios para configurar Audit Manager.

Registro para obtener una Cuenta de AWS

Si no dispone de una Cuenta de AWS, siga estos pasos para crear una.

Cómo registrarse en 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.

   Al registrarse en una Cuenta de AWS, se crea un Usuario raíz de la cuenta de AWS. 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 realizar tareas que requieran acceso de usuario raíz.

AWS le enviará un correo electrónico de confirmación luego de completar el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Crear un usuario administrativo

Después de registrarse para obtener una Cuenta de AWS, proteja su Usuario raíz de la cuenta de AWS, habilite AWS IAM Identity Center y cree un usuario administrativo para no utilizar el usuario raíz en las tareas cotidianas.

Protección de su Usuario raíz de la cuenta de AWS

1. Inicie sesión en la AWS Management Console como propietario de cuenta, elija Usuario raíz e ingrese el email de su Cuenta de AWS. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para 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 raíz de la Cuenta de AWS (consola) en la Guía del usuario de IAM.

Creación de un usuario administrativo

1. Activar IAM Identity Center

   Para obtener instrucciones, consulte Activación de AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center.
2. En IAM Identity Center, conceda acceso administrativo a un usuario administrativo.

Para ver un tutorial sobre cómo utilizar Directorio de IAM Identity Center como origen de identidad, consulte Configuración del acceso de usuarios con el Directorio de IAM Identity Center predeterminado en la Guía del usuario de AWS IAM Identity Center.

Cómo iniciar 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 IAM Identity Center.

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

Añada los permisos mínimos necesarios para acceder a Audit Manager y habilitarlo

Debe conceder a los usuarios los permisos necesarios para habilitar Audit Manager. Para los usuarios que necesitan acceso completo a Audit Manager, utilice la política administrada por AWSAuditManagerAdministratorAccess. Se trata de una política administrada por AWS disponible en su Cuenta de AWS, y es la política recomendada para los administradores de Audit Manager.

> **Tip**
>
> Como práctica recomendada de seguridad, le recomendamos que comience con las políticas administradas por AWS y, a continuación, avance hacia los permisos de privilegio mínimo. Las políticas administradas por AWS conceden permisos para muchos casos de uso comunes. Tenga presente que es posible que las políticas administradas de AWS no concedan permisos de privilegio mínimo para los casos de uso concretos, ya que están disponibles para que las utilicen todos los clientes de AWS. En consecuencia, se recomienda reducir aún más los permisos definiendo políticas administradas por el cliente específicas para sus casos de uso. Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de AWS Identity and Access Management.

Para dar acceso, añada permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.

- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones de Creación de un rol para un proveedor de identidades de terceros (federación) en la Guía del usuario de IAM.

- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Habilitar AWS Audit Manager

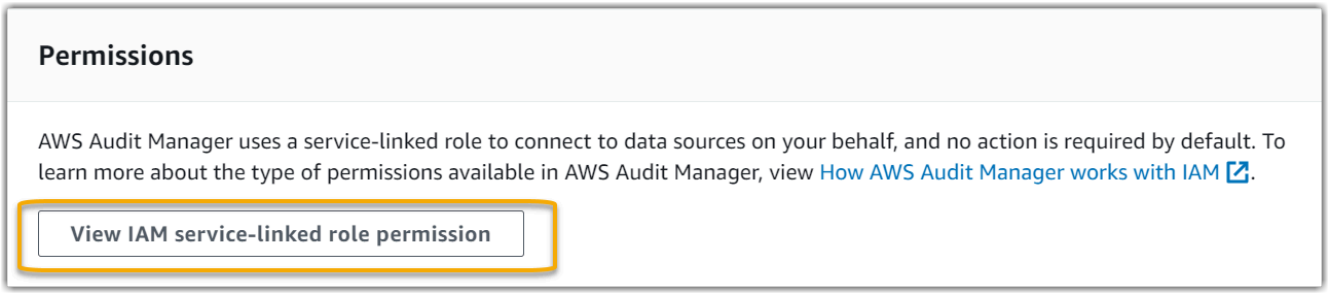
Puede habilitar Audit Manager usando la AWS Management Console, la API Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

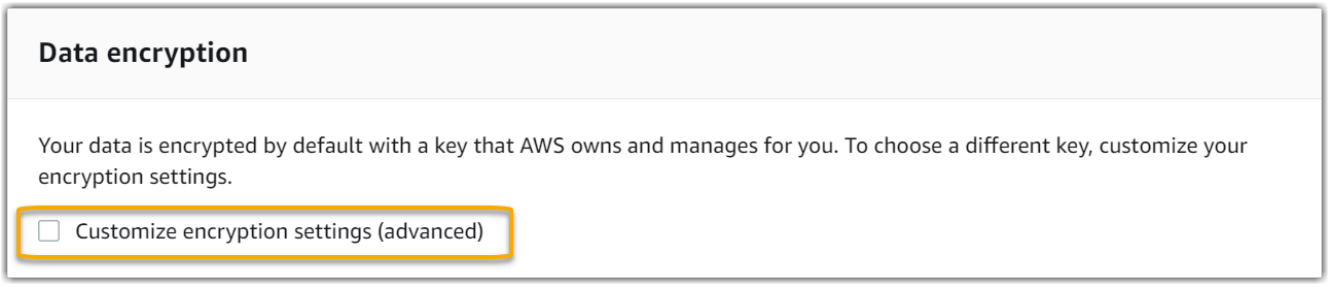
Habilitación del acceso de confianza mediante la consola Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. Utilice las credenciales de su identidad de IAM para iniciar sesión.
3. Elija Set up (Configurar)AWS Audit Manager.

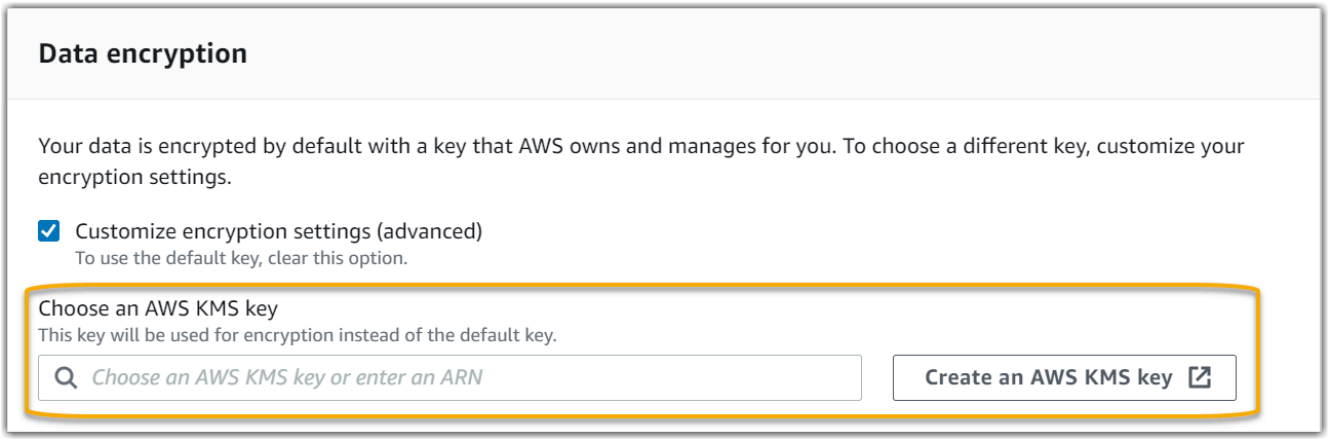
4. En Permisos, no es necesario realizar ninguna acción. Audit Manager utiliza un rol vinculado a servicio para conectarse a los orígenes de datos en su nombre. Para revisar el rol vinculado al servicio, seleccione Ver el permiso del rol vinculado al servicio de IAM.



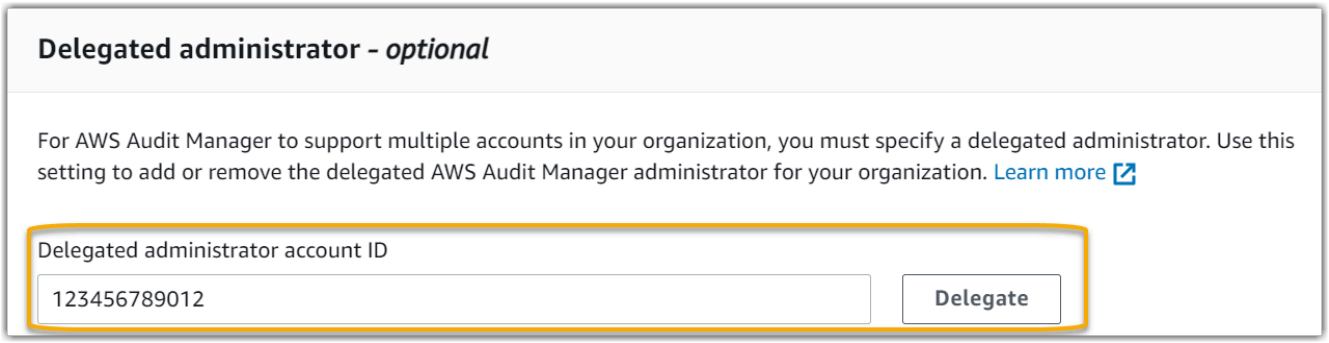
5. En Cifrado de datos, la opción predeterminada consiste en que Audit Manager cree y administre una y AWS KMS key para almacenar datos de forma segura.



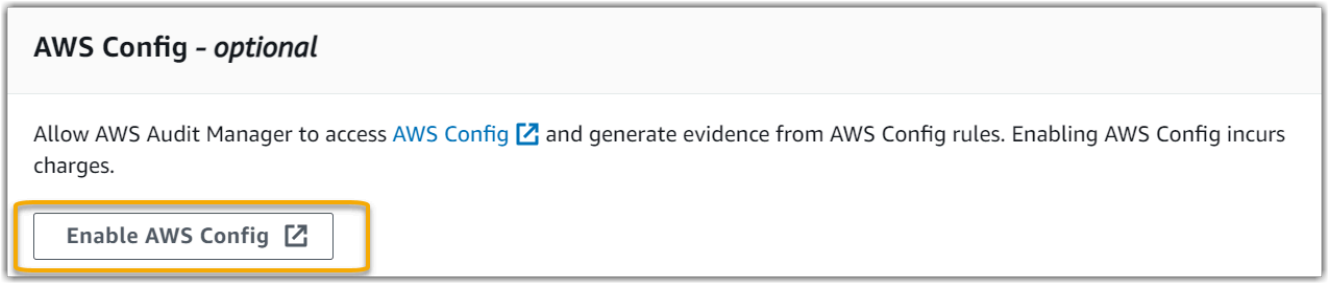
Si desea utilizar su propia clave administrada por el cliente para cifrar los datos en Audit Manager, marque la casilla de verificación situada junto a Personalizar la configuración de cifrado (avanzada). Puede elegir un par de claves KMS existente o crear una nueva.



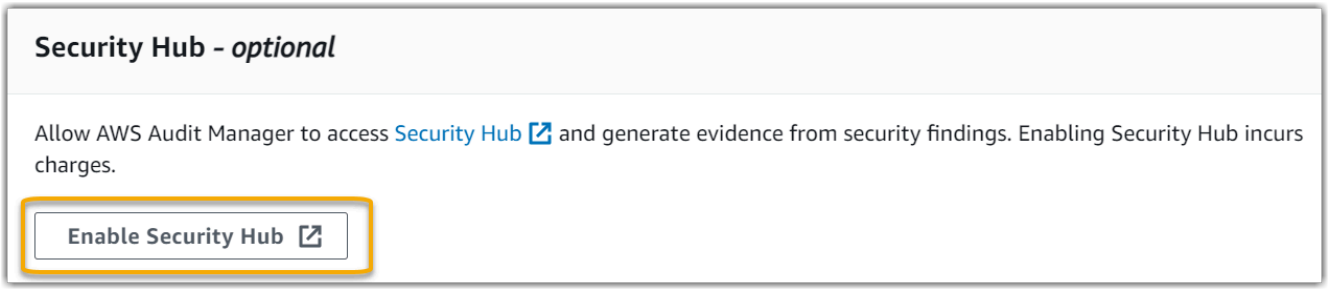
6. (Opcional) En Administrador delegado: opcional, puede especificar una cuenta de administrador delegado si desea que Audit Manager ejecute evaluaciones para varias cuentas. Para obtener más información y recomendaciones, consulte Habilitar y configurar AWS Organizations para su uso con Audit Manager.



7. (Opcional) En AWS Config: opcional, le recomendamos que habilite AWS Config para disfrutar de una experiencia óptima. Esto permite a Audit Manager generar evidencias mediante reglas de AWS Config. Para obtener más información y recomendaciones, consulte Habilitar y configurar AWS Config para su uso con Audit Manager.



8. (Opcional) Security Hub: le recomendamos que habilite Security Hub para disfrutar de una experiencia óptima. Esto permite a Audit Manager generar evidencias mediante comprobaciones de Security Hub. Para obtener más información y recomendaciones, consulte Habilitar y configurar AWS Security Hub para su uso con Audit Manager.



9. Seleccione Completar configuración para finalizar el proceso de configuración.

AWS CLI

Habilitación de Audit Manager mediante la AWS CLI

En la línea de comandos, ejecute el comando register-account con los siguientes parámetros de configuración:

- `--kms-key` (opcional): utilice este parámetro para cifrar sus datos de Audit Manager con su propia clave administrada por el cliente. Si no especifica ninguna opción aquí, Audit Manager creará y administrará una AWS KMS key en su nombre para el almacenamiento seguro de sus datos.
- `--delegated-admin-account` (opcional): utilice este parámetro para designar la cuenta de administrador delegado de su organización para Audit Manager. Si no especifica ninguna opción aquí, no se registrará ningún administrador delegado.

Ejemplo de entrada (sustituya el *texto del marcador de posición* por su propia información):

```
aws auditmanager register-account \
--kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
--delegated-admin-account 111122224444
```

Ejemplo de resultados:

```
{
    "status": "ACTIVE"
}
```

Para obtener más información sobre la AWS CLI y para obtener instrucciones sobre la instalación de herramientas de AWS CLI, consulte lo siguiente en la Guía de usuario de AWS Command Line Interface.

- Guía del usuario de la interfaz de la línea de comandos de AWS
- Configuración inicial de la AWS Command Line Interface

Audit Manager API

Habilitación de Audit Manager mediante la API de Audit Manager

Utilice la operación registerAccount con los siguientes parámetros de configuración:

- kmsKey (opcional): utilice este parámetro para cifrar sus datos de Audit Manager con su propia clave administrada por el cliente. Si no especifica ninguna opción aquí, Audit Manager creará y administrará una AWS KMS key en su nombre para el almacenamiento seguro de sus datos.
- delegatedAdminAccount (opcional): utilice este parámetro para especificar la cuenta de administrador delegado de su organización para Audit Manager. Si no especifica ninguna, no se registrará ningún administrador delegado.

Ejemplo de entrada (sustituya el *texto del marcador de posición* por su propia información):

```
{
    "kmsKey":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "delegatedAdminAccount":"111122224444"
}
```

Ejemplo de resultados:

```
{
  "status": "ACTIVE"
}
```

Recomendaciones

Para disfrutar al máximo de las prestaciones de Audit Manager, le recomendamos configurar las siguientes características y habilitar los siguientes Servicios de AWS.

Temas

- Configurar las características recomendadas de Audit Manager
- Configure las integraciones recomendadas con otros Servicios de AWS

Configurar las características recomendadas de Audit Manager

Tras habilitar Audit Manager, le recomendamos que habilite la característica de búsqueda de evidencias.

Buscador de evidencias proporciona una forma eficaz de buscar evidencias en Audit Manager. En lugar de explorar exhaustivamente carpetas de evidencias para encontrar lo que busca, puede utilizar el buscador de evidencias para consultarlas rápidamente. Si utiliza el buscador de evidencias como administrador delegado, puede buscar evidencias en todas las cuentas de miembros de su organización. Mediante una combinación de filtros y agrupaciones, puede reducir progresivamente el alcance de su consulta de búsqueda. Por ejemplo, si desea obtener una visión general del estado de su sistema, realice una búsqueda amplia y filtre por evaluación, intervalo de fechas y conformidad de los recursos. Si su objetivo es corregir un recurso específico, puede realizar una búsqueda restringida para encontrar evidencias que apunten a un identificador de control o recurso específico. Tras definir los filtros, puede agrupar y, a continuación, obtener una vista previa de los resultados de búsqueda coincidentes antes de crear un informe de evaluación.

Para utilizar el buscador de evidencias, debe habilitar esta característica en la configuración de Audit Manager. Para obtener más información, consulte Configuración del buscador de evidencias.

Configure las integraciones recomendadas con otros Servicios de AWS

Le recomendamos que habilite Servicios de AWS para lograr una experiencia óptima en Audit Manager:

- AWS Organizations: puede utilizar Organizaciones para ejecutar las evaluaciones de Audit Manager en varias cuentas y consolidar las evidencias en una cuenta de administrador delegado.
- AWS Security Hub y AWS Config: cuando habilita estos Servicios de AWS, se pueden utilizar como un tipo de origen de datos para los controles de sus evaluaciones de Audit Manager. Audit Manager puede informar de los resultados de las comprobaciones de conformidad directamente desde estos servicios.

Temas

Habilitar y configurar AWS Config (opcional)

Muchos controles de Audit Manager se utilizan AWS Config como tipo de origen de datos. Para permitir estos controles, debe habilitar AWS Config en todas las cuentas de cada Región de AWS en

la que Audit Manager esté habilitado. Si Audit Manager intenta recopilar evidencias para los controles que utilizan AWS Config como tipo de origen de datos y las reglas de AWS Config relacionadas no están habilitadas, no se recopilará ninguna evidencia para esos controles.

Audit Manager no administra AWS Config para usted. Puede seguir estos pasos para habilitar AWS Config y configurar sus ajustes.

Tareas para integrar AWS Config con Audit Manager

- Paso 1: Habilite AWS Config
- Paso 2: configure sus ajustes de AWS Config para utilizarlos con Audit Manager

Paso 1: Habilite AWS Config

Puede habilitar AWS Config con la AWS Config la consola o la API. Para obtener instrucciones, consulte Introducción a AWS Config en la Guía para desarrolladores de AWS Config.

Paso 2: configure sus ajustes de AWS Config para utilizarlos con Audit Manager

> **Important**
>
> Habilitar AWS Config es una recomendación opcional. Sin embargo, si habilitaAWS Config, se requieren los siguientes ajustes.

Una vez habilitado AWS Config, asegúrese también de habilitar las reglas de AWS Config o implementar un paquete de conformidad para la norma de conformidad relacionada con la auditoría. Este paso garantiza que Audit Manager pueda importar los resultados de las reglas de AWS Config que haya habilitado.

Después de habilitar una regla de AWS Config, le recomendamos que revise los parámetros de dicha regla. A continuación, debe validar dichos parámetros con respecto a los requisitos del marco de conformidad que haya elegido. Si es necesario, puede actualizar los parámetros de una regla en AWS Config para asegurarse de que se ajusta a los requisitos del marco. Esto ayudará a garantizar que sus evaluaciones recopilen las evidencias de control de conformidad correctas para un marco determinado.

Supongamos, por ejemplo, que está creando una evaluación para CIS v1.2.0. Este marco tiene un control denominado 1.4: asegúrese de que las claves de acceso se roten cada 90 días o menos.

En AWS Config, la regla access-keys-rotated tiene un parámetro `maxAccessKeyAge` con un valor predeterminado de 90 días. Por lo tanto, la regla concuerda con los requisitos de control establecidos. Si no utiliza el valor predeterminado, asegúrese de que sea igual o superior al requisito de 90 días establecido en la versión 1.2.0 del CIS.

Puede encontrar los datos relativos a los parámetros predeterminados de cada regla administrada en la AWS Config documentación. Para obtener instrucciones sobre cómo habilitar o configurar una regla, consulte Trabajar con las reglas administradas de AWS Config.

Habilitar y configurar AWS Security Hub (opcional)

Muchos controles de Audit Manager utilizan Security Hub como tipo de origen de datos. Para permitir estos controles, debe habilitar Security Hub en todas las cuentas de cada región en la que Audit Manager esté habilitado. Si Audit Manager intenta recopilar evidencias para los controles que utilizan Security Hub como tipo de origen de datos y las reglas de Security Hub relacionadas no están habilitadas, no se recopilará ninguna evidencia para esos controles.

Audit Manager no administra Security Hub por usted. Puede seguir estos pasos para habilitar Security Hub y configurar sus ajustes.

Tareas para integrar AWS Security Hub con Audit Manager

- Paso 1: Habilite AWS Security Hub
- Paso 2: configure sus ajustes de Security Hub para utilizarlos con Audit Manager

Paso 1: Habilite AWS Security Hub

Puede habilitar Security Hub mediante la consola o la API. Para conocer las instrucciones, consulte Configuración de AWS Security Hub en la Guía del usuario de AWS Security Hub.

Paso 2: configure sus ajustes de Security Hub para utilizarlos con Audit Manager

> **Important**
>
> Habilitar el Security Hub es una recomendación opcional. Sin embargo, si habilita Security Hub, deberá realizar los siguientes ajustes.

Después de habilitar Security Hub, asegúrese de hacer lo siguiente:

- Habilitar AWS Config y configurar el registro de recursos: Security Hub utiliza reglas de AWS Config vinculadas a servicios para realizar la mayoría de los controles de seguridad de los controles. Para poder utilizar dichos controles, AWS Config debe estar habilitado y configurado para registrar los recursos necesarios para los controles que haya habilitado en cada estándar habilitado.
- Habilitar todos los estándares de seguridad: este paso garantiza que Audit Manager pueda importar los resultados de todos los estándares de conformidad compatibles.
- Habilitar la configuración de resultados de control consolidados en Security Hub: esta configuración está activada de forma predeterminada si habilitó el Centro de seguridad a partir del 23 de febrero de 2023.

> **Note**
>
> Cuando habilita los resultados consolidados, Security Hub genera un único resultado para cada control de seguridad (incluso cuando se utiliza el mismo control en varios estándares). Cada resultado de Security Hub se recopila como una evaluación de recursos única en Audit Manager. En consecuencia, los resultados consolidados revelan una disminución del total de evaluaciones de recursos únicos que Audit Manager realiza para los resultados de Security Hub. Por esta razón, el uso de resultados consolidados a menudo puede resultar en una reducción de los costes de uso de Audit Manager. Para obtener más información sobre el uso de Security Hub como tipo de origen de datos, consulte AWS Security Hub controles compatibles con AWS Audit Manager. Para obtener más información acerca de los precios, consulte Precios de AWS Audit Manager.

Si utiliza AWS Organizations y quiere recopilar evidencias de Security Hub de sus cuentas de miembros, también debe realizar los siguientes pasos en Security Hub.

Para configurar los ajustes de Security Hub de su organización

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Security Hub en https://console.aws.amazon.com/securityhub/.
2. Con su cuenta de administración de AWS Organizations, designe una cuenta como administrador delegado de Security Hub. Para obtener información, consulte Designación de una cuenta de administrador de Security Hub en la Guía del usuario de AWS Security Hub.

> **Note**
>
> Asegúrese de que la cuenta de administrador delegado que designe en Security Hub sea la misma que utiliza en Audit Manager.

3. Con su cuenta de administrador delegado de organizaciones, vaya a Configuración, Cuentas, seleccione todas las cuentas y, a continuación, agréguelas como miembros seleccionando Inscripción automática. Para obtener más información, consulte Habilitar una cuenta miembro de la organización en la Guía del usuario de AWS Security Hub.
4. Active AWS Config para cada cuenta de miembro de la organización. Para obtener más información, consulte Habilitar una cuenta miembro de la organización en la Guía del usuario de AWS Security Hub.
5. Active el estándar de seguridad PCI DSS para cada cuenta miembro de la organización. El estándar del indicador de referencia de CIS AWS Foundations y el estándar de mejores prácticas fundamentales de AWS, ya están activados de forma predeterminada. Para obtener más información sobre este estándar, consulte Habilitar el estándar de seguridad en la Guía del usuario de AWS Security Hub.

Habilitar AWS Organizations (opcional)

Audit Manager admite varias cuentas mediante la integración con AWS Organizations. Audit Manager puede ejecutar las evaluaciones en varias cuentas y consolidar las evidencias en una cuenta de administrador delegado. El administrador delegado tiene permisos para crear y administrar recursos de Audit Manager con la organización como zona de confianza. Solo la cuenta de administración puede agregar un administrador delegado.

Tareas para integrar AWS Organizations con Audit Manager

- Paso 1: crear o unirse a una organización
- Paso 2: Habilitar todas las características en la organización.
- Paso 3: especificar un administrador delegado para Audit Manager

Paso 1: crear o unirse a una organización

Si su Cuenta de AWS no forma parte de una organización, puede crearla o unirse a ella. Para obtener instrucciones sobre cómo hacerlo, consulte Creación y administración de una organización en la Guía del usuario de AWS Organizations.

Paso 2: Habilitar todas las características en la organización.

A continuación, debe habilitar todas las características en la organización. Para obtener más información, consulte Habilitar todas las características en la organización en la Guía del usuario de AWS Organizations.

Paso 3: especificar un administrador delegado para Audit Manager

Le recomendamos que habilite Audit Manager mediante una cuenta de administración de organizaciones y, a continuación, especifique un administrador delegado. Después, puede usar la cuenta de administrador delegado para iniciar sesión y ejecutar las evaluaciones. Como práctica recomendada, aconsejamos que cree evaluaciones únicamente con la cuenta de administrador delegado en lugar de la cuenta de administración.

> **Warning**
>
> Después de especificar un administrador delegado mediante una cuenta de administración de organizaciones, su cuenta de administración ya no podrá crear evaluaciones adicionales en Audit Manager. Además, la recopilación de evidencias se detiene para cualquier evaluación existente creada por la cuenta de administración. Audit Manager recopila y adjunta evidencias a la cuenta de administrador delegado, que es la cuenta principal para gestionar las evaluaciones de la organización.

Para añadir o cambiar un administrador delegado después de habilitar Audit Manager, consulte Configuración de AWS Audit Manager, Administrador delegado.

Cuestiones que se deben tener en cuenta:

- No puede usar su cuenta de administración como administrador delegado en Audit Manager.
- Si desea habilitar Audit Manager en más de una Región de AWS, debe designar una cuenta de administrador delegado por separado en cada región. En la configuración de Audit Manager, debe designar la misma cuenta de administrador delegado en todas las regiones.

- Si proporcionó una clave administrada por el cliente al habilitar Audit Manager, asegúrese de que la cuenta de administrador delegado tenga acceso a esa clave de KMS. Para revisar y cambiar la configuración del cifrado de Audit Manager, consulte Cifrado de datos.
- Para obtener soluciones a los problemas comunes de las organizaciones y los administradores delegados en Audit Manager, consulte Solución de problemas AWS Organizations y del administrador delegado.

¿Qué tengo que hacer ahora?

Ahora que ha configurado Audit Manager, está listo para empezar a utilizar el servicio. También puede visitar la página de configuración de la consola para actualizar cualquier configuración que haya elegido al configurar Audit Manager.

Introducción a Audit Manager

Puede empezar a utilizar Audit Manager siguiendo un tutorial que le explica cómo crear su primera evaluación. Para obtener más información, consulte el Tutorial para propietarios de auditorías: crear una evaluación.

Actualice la configuración de Audit Manager

Puede actualizar la configuración en cualquier momento. Para obtener más información, consulte Configuración de AWS Audit Manager.

Introducción a AWS Audit Manager

Utilice los tutoriales paso a paso de esta sección para aprender a realizar tareas con AWS Audit Manager.

Tip

Los siguientes tutoriales están clasificados por audiencia. Elija el tutorial adecuado para usted dependiendo de su función como propietario de la auditoría o delegado.

- Los propietarios de las auditorías son usuarios de Audit Manager responsables de crear y gestionar las evaluaciones. En el mundo empresarial, los responsables de las auditorías suelen ser profesionales del gobierno, la gestión de riesgos y el cumplimiento (GRC). Sin embargo, en el contexto de Audit Manager, las personas de los equipos de SecOps o DevOps también pueden asumir el papel de usuario propietario de una auditoría. Los responsables de la auditoría pueden solicitar la ayuda de un experto en la materia (también denominado delegado) para revisar controles específicos y validar las pruebas. Los propietarios de la auditoría deben tener los permisos necesarios para gestionar una evaluación.
- Los delegados son expertos en la materia con experiencia técnica o empresarial especializada. Aunque no son propietarios ni gestionan las evaluaciones de Audit Manager, pueden contribuir a ellas. Los delegados ayudan a los responsables de las auditorías en tareas como la validación de las pruebas para los controles que entran dentro de su área de especialización. Los delegados tienen permisos limitados en Audit Manager. Esto se debe a que los propietarios de las auditorías delegan la revisión de conjuntos de control específicos y no de las evaluaciones completas.

Para obtener más información sobre estas personas y otros conceptos de Audit Manager, consulte propietarios de la auditoría y delegados en la sección Conceptos y terminología de AWS Audit Manager de esta guía. Para obtener más información sobre los permisos de IAM recomendados para cada persona, consulte Políticas recomendadas para los usuarios de AWS Audit Manager.

Tutoriales de Audit Manager

Creación de una evaluación

Público: propietarios de auditorías

Descripción general: Siga las instrucciones paso a paso para crear su primera evaluación y empezar a utilizarla rápidamente. Este tutorial explica cómo utilizar un marco estándar para crear una evaluación y comenzar la recopilación automática de pruebas.

Revisión de un conjunto de controles

Público: delegados

Descripción general: ayude al propietario de una auditoría revisando las pruebas para detectar los controles que entran dentro de su área de especialización. Aprenda a revisar los conjuntos de controles y sus pruebas relacionadas, añada comentarios, cargue pruebas adicionales y actualice el estado de un control.

Tutorial para propietarios de auditorías: crear una evaluación

En este tutorial, solo se proporciona una introducción a AWS Audit Manager. En este tutorial, creará una evaluación utilizando el marco AWS Audit Manager de muestra. Al crear una evaluación, se inicia el proceso continuo de recopilación automática de pruebas para los controles de ese marco.

Este tutorial le enseña a realizar las siguientes tareas:

- Seleccione un marco estándar a partir del cual crear una evaluación
- Especifique las cuentas de AWS que desee incluir en la evaluación
- Especifique los servicios de AWS que desee incluir en la evaluación
- Especifique los propietarios de la auditoría para su evaluación
- Revise y cree su evaluación

Antes de comenzar este tutorial, asegúrese de cumplir las siguientes condiciones:

- Ha completado todos los requisitos previos que se describen en Configuración de AWS Audit Manager. Debe usar su cuenta de AWS y la consola de AWS Audit Manager para completar este tutorial.

- Su identidad de IAM cuenta con los permisos adecuados para crear y gestionar una evaluación en AWS Audit Manager. Las dos políticas sugeridas para conceder estos permisos son el Ejemplo 2: permitir el acceso total del administrador y el Ejemplo 3: permitir el acceso de la administración.
- Está familiarizado con la terminología y la funcionalidad de Audit Manager. Para obtener información general acerca, consulte¿Qué es AWS Audit Manager? y Conceptos y terminología de AWS Audit Manager.

> **Note**
>
> AWS Audit Manager ayuda a recopilar evidencias relevantes para verificar el cumplimiento de estándares y reglamentos de cumplimiento específicos. Sin embargo, no evalúa el cumplimiento en sí mismo. Por lo tanto, es posible que las pruebas recopiladas mediante AWS Audit Manager no incluyan toda la información sobre su uso de AWS que se necesita para las auditorías. AWS Audit Manager no sustituye a los asesores legales ni a los expertos en cumplimiento.

Paso 1: especificar los detalles de la evaluación

Como primer paso, seleccione un marco y proporcione información básica para la evaluación.

Pasos para especificar los detalles de la evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. Elija LaunchAWS Audit Manager.
3. En el panel de navegación, elija Primeros pasos y, a continuación, elija Iniciar con un marco.
4. Elija el marco que desee y, a continuación, elija Crear evaluación a partir del marco. En este ejemplo se utiliza el AWS Audit ManagerMarco de muestra.
5. En Nombre de la evaluación, escriba un nombre para su evaluación.
6. (Opcional) En Descripción de la evaluación, escriba una descripción para su evaluación.
7. En Destino de los informes de evaluación, elija el bucket de Amazon S3 en el que desee guardar los informes de evaluación.
8. En Marcos, confirme que ha seleccionado AWS Audit ManagerMarco de ejemplo (o el marco que prefiera).

9. En Etiquetas, elija Añadir nueva etiqueta para asociar una etiqueta a su evaluación. Puede especificar una clave y un valor para cada etiqueta. La clave de etiqueta es obligatoria y se puede utilizar como criterio de búsqueda al buscar esta evaluación. Para obtener más información sobre las etiquetas de AWS Audit Manager, consulte Etiquetado de recursos de AWS Audit Manager.
10. Elija Siguiente.

Paso 2: especificar las cuentas de AWS en el ámbito

A continuación, especifique las cuentas de AWS que desea incluir en el alcance de su evaluación.

AWS Audit Managerse integra conAWS Organizations, por lo que puede ejecutar una evaluación de Audit Manager en varias cuentas y consolidar las pruebas en una cuenta de administrador delegado. Para habilitar organizaciones en Audit Manager (si aún no lo ha hecho), consulte Habilitar AWS Organizations (opcional) en la página de configuración de esta guía.

> **Note**
>
> Audit Manager puede admitir hasta aproximadamente 150 cuentas de miembros en el ámbito de una sola evaluación. Si intenta incluir más de 150 cuentas, es posible que no se pueda crear la evaluación.

Para especificar las cuentas incluidas en el ámbito

1. En cuentas de AWS, seleccione las cuentas de AWS que desee incluir en el ámbito de la evaluación.
   - Si ha activado organizaciones en AWS Audit Manager, se muestran varias cuentas.
   - Si no activó organizaciones en Audit Manager, solo aparecerá su cuenta actual.
2. Elija Siguiente.

Paso 3: especificar los servicios de AWS incluidos en el ámbito

El marco que seleccionó anteriormente define los servicios de AWS que Audit Manager supervisa y para los que recopila pruebas.

Cuando utiliza la consola Audit Manager para crear una evaluación a partir de un marco estándar, la lista de servicios incluidos en el ámbito de aplicación se preselecciona y no se puede editar. Esto se debe a que Audit Manager asigna y selecciona automáticamente el origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco estándar. Si no se selecciona un servicio de AWS de la lista, Audit Manager no recopila pruebas de los recursos relacionados con ese servicio. Este también es el caso si está seleccionado pero no se ha suscrito a él en su entorno.

En este paso del tutorial, puede revisar qué servicios de AWS están incluidos en el ámbito de la evaluación en función de la definición del marco. Para obtener más información sobre los marcos y cómo acceder a ellos y revisarlos, consulte la sección Biblioteca de marcos de esta guía.

Para especificar los servicios de AWS incluidos en su ámbito

1. Revise en la sección de servicios de AWS la lista de servicios incluidos en el ámbito de esta evaluación.
2. Elija Siguiente.

> **Tip**
>
> Si necesita editar la lista de servicios incluidos en el ámbito, puede hacerlo mediante la API CreateAssessment que proporciona Audit Manager.
> Como alternativa, puede personalizar un marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Paso 4: Especificar los responsables de la auditoría

En este paso, especifique quiénes son los responsables de la auditoría en la evaluación. Los responsables de la auditoría son las personas de su empresa u organización (normalmente de los equipos de GRC, SecOps o DevOps) que se encargan de gestionar la evaluación de Audit Manager. Se recomienda que utilicen la política AWSAuditManagerAdministratorAccess.

Pasos para especificar los responsables de la auditoría

1. En Propietarios de la auditoría, elija a los propietarios de la auditoría para su evaluación. Para encontrar más propietarios de auditorías, utilice la barra de búsqueda para buscar por nombre o cuenta de AWS.

2. Elija Siguiente.

Paso 5: Revisar y crear

Revise de la información de su evaluación. Para modificar la información de un paso, seleccione Editar. Cuando haya terminado, elija Crear evaluación para iniciar su primera evaluación e iniciar la recopilación continua de pruebas.

Tras crear una evaluación, la recopilación de evidencias continúa hasta que el estado de la evaluación cambia a inactiva. También puede detener la recopilación de evidencias para un control específico cambiando el estado del control a inactivo.

> **Note**
>
> Las pruebas automatizadas están disponibles 24 horas después de crear la evaluación. AWS Audit Manager recopila automáticamente pruebas de varias fuentes de datos, y la frecuencia de esa recopilación de pruebas se basa en el tipo de prueba. Para obtener más información, consulte la sección Frecuencia de recolección de evidencias de esta guía.

¿Qué tengo que hacer ahora?

Le recomendamos que continúe profundizando en los conceptos y las herramientas presentados en este tutorial. Para ello, consulte los siguientes recursos:

- Revisión de las evaluaciones: Le presenta la página de evaluación, donde puede explorar los diferentes componentes de su evaluación.
- Evaluaciones en AWS Audit Manager: Se basa en este tutorial y proporciona información detallada sobre los conceptos y las tareas de la gestión de una evaluación. En este documento, le recomendamos, sobre todo, que consulte los siguientes temas:
  - ¿Cómo crear una evaluación desde un marco diferente?
  - ¿Cómo revisar la prueba de una evaluación y generar un informe de evaluación?
  - ¿Cómo cambiar el estado de una evaluación o eliminarla?
- Biblioteca de marcos: Presenta la biblioteca de marcos y explica cómo crear un marco personalizado para sus propias necesidades de cumplimiento específicas.

- Biblioteca de control: Presenta la biblioteca de controles y explica cómo crear un control personalizado para usarlo en su marco personalizado.
- Conceptos y terminología de AWS Audit Manager: Proporciona definiciones de los conceptos y la terminología utilizados en Audit Manager.
- [Vídeo] Recopile pruebas y gestione los datos de auditoría medianteAWS Audit Manager : muestra el proceso de creación de la evaluación que se describe en este tutorial y otras tareas, como la revisión de un control y la generación de un informe de evaluación.

Tutorial para delegados: Revisión de un conjunto de controles

En este tutorial se describe cómo revisar un conjunto de controles que el propietario de una auditoría compartió con usted en AWS Audit Manager.

Los propietarios de las auditorías utilizan Audit Manager para crear evaluaciones y recopilar pruebas para los controles enumerados en esa evaluación. A veces, los propietarios de las auditorías pueden tener dudas o necesitar ayuda a la hora de validar la prueba de un conjunto de controles. En esta situación, el propietario de una auditoría puede delegar un conjunto de controles en un experto en la materia para su revisión.

Como delegado, usted ayuda a los responsables de la auditoría a revisar las pruebas recopiladas para detectar los controles que entran dentro de su área de especialización.

Este tutorial le enseña a realizar las siguientes tareas:

- Acceder a las notificaciones que le envíe el propietario de la auditoría
- Revisar un conjunto de controles y su prueba relacionada
- Cargar pruebas manuales que respalden un control
- Agregar un comentario para un control que estés revisando
- Actualizar el estado de un control
- Envíe el conjunto de controles revisado al propietario de la auditoría cuando finalice la revisión

Antes de comenzar este tutorial, asegúrese de cumplir las siguientes condiciones:

- Su cuenta de AWS está configurada. Para completar este tutorial, asegúrese de que utiliza su cuenta de AWS y la consola de AWS Audit Manager. Para obtener más información, consulte Configuración de AWS Audit Manager.

- Está familiarizado con la terminología y la funcionalidad de Audit Manager. Para obtener una descripción general de Audit Manager, consulte ¿Qué es AWS Audit Manager? y Conceptos y terminología de AWS Audit Manager.

Paso 1: acceder a las notificaciones

Comience por iniciar sesión en AWS Audit Manager, donde podrá acceder a sus notificaciones para ver los conjuntos de controles que se le han delegado para su revisión.

Para acceder a las notificaciones

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija Notificaciones. O bien, en la barra parpadeante azul en la parte superior de la página, elija Ver notificación para abrir la página de notificaciones.
3. En la página de Notificaciones, puede revisar la lista de conjuntos de controles que se le han delegado. La tabla de notificaciones incluye la siguiente información:
   - Fecha: la fecha en la que se delegó el conjunto de controles.
   - Evaluación: el nombre de la evaluación asociada al conjunto de controles. Puede elegir un nombre para la evaluación para abrir la página de detalles de la evaluación.
   - Conjunto de controles: el nombre del conjunto de controles que se le ha delegado para su revisión.
   - Origen: el usuario o rol que le delegó el conjunto de controles.
   - Descripción: las instrucciones de revisión proporcionadas por el propietario de la auditoría.

> **Tip**
>
> También puede suscribirse a un tema de SNS para recibir alertas por correo electrónico cuando se le asigne un conjunto de controles para su revisión. Para obtener más información, consulte Notificaciones de AWS Audit Manager.

Paso 2: revisar el conjunto de controles y la prueba relacionada

El siguiente paso es revisar los conjuntos de control que el propietario de la auditoría le ha delegado. Al examinar los controles y sus pruebas, puede determinar si es necesaria alguna acción adicional para realizar un control. Las acciones adicionales pueden incluir cargar manualmente pruebas adicionales para demostrar conformidad o dejar un comentario sobre ese control.

Para revisar un conjunto de controles

1. Revise en la página de Notificaciones la lista de conjuntos de controles que se le han delegado. A continuación, identifique cuál desea revisar y elija el nombre de la evaluación relacionada.
2. En la pestaña Controles de la página de detalles de la evaluación, desplácese hacia abajo hasta la tabla de Conjuntos de controles.
3. En la columna Controles agrupados por conjunto, expanda el nombre de un conjunto de controles para mostrar sus controles. A continuación, elija el nombre de un control para abrir la página de detalles del control.
4. (Opcional) Seleccione Actualizar el estado del control para cambiar el estado del control. Mientras la revisión esté en curso, puede marcar el estado como En revisión.
5. Revise la información sobre el control en las pestañas de Carpetas de pruebas, Orígenes de datos, Comentarios y Registro de cambios. Para obtener más información sobre cada una de estas pestañas y cómo interpretar los datos que contienen, consulte Revisar los controles de una evaluación.

Para revisar la prueba de un control

1. En la página de detalles del control, seleccione la pestaña Carpetas de pruebas.
2. Navegue hasta la tabla de Carpetas de pruebas, donde se muestra una lista de carpetas que contienen las pruebas de ese control. Estas carpetas se organizan y nombran en función de la fecha en que se recopilaron las pruebas contenidas en esa carpeta.
3. Elija el nombre de una carpeta de evidencias para abrirla. Desde aquí, puede revisar un resumen de todas las pruebas recopiladas en esa fecha. Este resumen también incluye el número total de problemas relacionados con la verificación de la conformidad que se notificaron directamente desde AWS Security Hub, AWS Config o ambos. Para obtener instrucciones sobre cómo interpretar los datos de esta página, consulte Revisión de las carpetas de pruebas.

4. En la página de resumen de la carpeta de pruebas, navegue hasta la tabla de Pruebas. En la columna Tiempo, selecciona una línea para abrir y revisar los detalles de las pruebas recopiladas en ese momento. Para obtener instrucciones sobre cómo interpretar los datos de una página de detalles de las evidencias, consulte Revisión de las evidencias individuales.

Paso 3. Cargue pruebas manuales (opcional)

Aunque AWS Audit Manager recopila pruebas automáticamente para muchos controles, en algunos casos es posible que deba proporcionar pruebas adicionales. En estos casos, puede cargar manualmente pruebas que le ayuden a demostrar la conformidad de ese control.

Antes de poder cargar pruebas manuales para su evaluación, primero debe colocarlas en un bucket de S3. Para ver las instrucciones de carga, consulte Creación de una bucket y Carga de objetos en la Guía del usuario de Amazon Simple Storage Service.

> **Important**
>
> Cada cuenta de AWS solo puede cargar manualmente hasta 100 archivos de pruebas a un control cada día. Si se supera esta cuota diaria, no se podrá realizar ninguna carga manual adicional en ese control. Si necesita cargar una gran cantidad de evidencias manuales en un solo control, hágalo en lotes durante varios días.

Para cargar pruebas manuales que respalden un control

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En la página de Notificaciones, puede ver la lista de conjuntos de controles que se le han delegado. Identifique el conjunto de controles para el que desea añadir pruebas y elija el nombre de la evaluación relacionada para abrir la página de detalles de la evaluación.
3. Seleccione la pestaña Controles, desplácese hacia abajo hasta Conjuntos de controles y, a continuación, seleccione el nombre de un control para abrirlo.
4. Seleccione la pestaña Carpetas de pruebas y, a continuación, elija Cargar pruebas manuales.
5. En la siguiente página, ingrese el S3 URI de la prueba. Para encontrar el URI de S3, vaya al objeto en la consola de Amazon S3 y elija Copiar URI de S3.
6. Elija Cargar para cargar las pruebas manuales.

> **Note**
>
> Cuando un control está inactivo, no puede cargar pruebas manuales para ese control. Para cargar pruebas manuales, primero debe cambiar el estado del control a en revisión o revisado. Para obtener instrucciones sobre cómo cambiar el estado de un control, consulte Paso 5: marcar un control como revisado (opcional).

Paso 4. Añada un comentario para un control (opcionalmente).

Puede añadir comentarios a cualquier control que revise. El propietario de la auditoría puede ver estos comentarios. Por ejemplo, puede dejar un comentario para proporcionar una actualización de estado y confirmar que ha solucionado cualquier problema relacionado con ese control.

Para añadir un comentario a un control

1. Revise en la página de Notificaciones la lista de conjuntos de controles que se le han delegado. Busque el conjunto de controles para el que desea dejar un comentario y elija el nombre de la evaluación relacionada.
2. Seleccione la pestaña Controles, desplácese hacia abajo hasta la tabla de Conjuntos de controles y, a continuación, seleccione el nombre de un control para abrirlo.
3. Seleccione la pestaña Comentarios.
4. En Enviar comentarios, introduzca su comentario en el cuadro de texto.
5. Seleccione Enviar comentario para añadir su comentario. Su comentario aparece ahora en la sección de Comentarios anteriores de la página, junto con cualquier otro comentario relacionado con este control.

Paso 5: marcar un control como revisado (opcional)

Cambiar el estado de un control es opcional. Sin embargo, le recomendamos que cambie el estado de cada control a Revisado a medida que complete la revisión de ese control. Independientemente del estado de cada control individual, puede enviar los controles al propietario de la auditoría.

Para marcar un control como revisado

1. Revise en la página de Notificaciones la lista de conjuntos de controles que se le han delegado. Busque el conjunto de controles que contiene el control que desea marcar como revisado. A

continuación, elija el nombre de la evaluación relacionada para abrir la página de detalles de la evaluación.

2. En la pestaña Controles de la página de detalles de la evaluación, desplácese hacia abajo hasta la tabla de Conjuntos de controles.
3. En la columna Controles agrupados por conjunto, expanda el nombre de un conjunto de controles para mostrar sus controles. Elija el nombre de un control para abrir la página de detalles del control.
4. Seleccione Actualizar el estado del control y cambie el estado a Revisado.
5. En la ventana emergente que aparece, seleccione Actualizar el estado del control para confirmar que ha terminado de revisar el control.

Paso 6. Volver a enviar el conjunto de controles revisado al propietario de la auditoría

Cuando haya terminado de revisar todos los controles, devuelva el conjunto de controles al propietario de la auditoría para que sepa que ha finalizado la revisión.

Para volver a enviar un conjunto de controles revisado al propietario

1. Revise en la página de Notificaciones la lista de conjuntos de controles que se le asignaron. Busque el conjunto de controles que desea enviar al propietario de la auditoría y elija el nombre de la evaluación relacionada.
2. Desplácese hacia abajo hasta la tabla de Conjuntos de controles, seleccione el conjunto de controles que desee devolver al propietario de la auditoría y, a continuación, seleccione Enviar a revisión.
3. En la ventana emergente que aparece, puede añadir cualquier comentario de alto nivel sobre ese conjunto de controles antes de seleccionar Enviar para su revisión.

Tras enviar el control al propietario de la auditoría, el propietario de la auditoría podrá ver cualquier comentario que le haya dejado.

¿Qué tengo que hacer ahora?

Puede seguir aprendiendo más sobre los conceptos que se presentan en este tutorial. A continuación se presentan algunos recursos recomendados:

- Revisión de las evaluaciones: le presenta la página de evaluación, en la que puede explorar los diferentes componentes de una evaluación de AWS Audit Manager.
- Revisar los controles de una evaluación y Revisar las pruebas de una evaluación: proporcionan definiciones de datos que le ayudarán a interpretar los controles y las pruebas de cada evaluación.
- Conceptos y terminología de AWS Audit Manager: proporciona definiciones de los conceptos y la terminología que se utilizan en Audit Manager.

Uso del panel de control de Audit Manager

Con el panel de control de Audit Manager, puede visualizar las evidencias no conformes en sus evaluaciones activas. Es una forma cómoda y rápida de supervisar sus evaluaciones, mantenerse informado y solucionar los problemas de forma proactiva. De forma predeterminada, el panel proporciona una vista agregada de arriba hacia abajo de todas las evaluaciones activas. Con esta vista, puede identificar visualmente los problemas en sus evaluaciones sin tener que examinar primero una gran cantidad de evidencias individuales.

El panel de control es la primera pantalla que aparece al iniciar sesión en la consola de Audit Manager. Contiene dos widgets que muestran los datos y los indicadores clave de rendimiento (KPI) que son más relevantes para usted. Con un filtro de evaluación, puede refinar estos datos para centrarse en los KPI de una evaluación específica. A partir de ahí, puede revisar las agrupaciones de dominios de control para identificar qué controles tienen la mayor cantidad de evidencias no conformes. A continuación, puede explorar los controles subyacentes para examinar y solucionar los problemas.

> **Note**
>
> Si es la primera vez que utiliza Audit Manager o no tiene ninguna evaluación activa, no se mostrará ningún dato en el panel de control. Para empezar, cree una evaluación. Esto inicia la recopilación continua de evidencias. Después de un período de 24 horas, los datos de evidencia agregados comenzarán a aparecer en el panel de control. Puede leer las siguientes secciones para aprender a entender e interpretar estos datos.

Esta página abarca los siguientes temas:

Temas

Conceptos y terminología del panel

En esta sección se describen aspectos importantes que debe conocer sobre el panel de control de Audit Manager antes de empezar a usarlo.

Permisos y visibilidad

Tanto los propietarios de la auditoría como los delegados tienen acceso al panel de control. Esto significa que ambas personas pueden ver las métricas y los agregados de todas las evaluaciones activas de su cuenta AWS. Tener acceso a la misma información permite a todo su equipo centrarse en los mismos KPI y objetivos.

Filtros

Audit Manager proporciona un nivel de página the section called “Filtro de evaluación” que puede aplicar a todos los widgets de su panel de control.

Evidencias no conformes

El panel destaca los controles de sus evaluaciones que contienen evidencias de verificación de la conformidad con una conclusión no conforme. Las evidencias de las comprobaciones de conformidad se refieren a los controles que utilizan AWS Config o AWS Security Hub como un tipo de origen de datos. Para este tipo de evidencia, Audit Manager informa del resultado de una verificación de conformidad directamente desde esos servicios. Si el Centro de seguridad informa de un resultado fallido o AWS Config informa de un resultado no conforme, Audit Manager clasifica las evidencias como no conformes.

Evidencia no concluyente

Las evidencias son no concluyentes si una verificación de cumplimiento no está disponible o no es aplicable. Como resultado, no se puede realizar ninguna evaluación del cumplimiento. Este es el caso si un control usa AWS Config o AWS Security Hub como un tipo de origen de datos, pero usted no habilitó esos servicios. Este también es el caso si el control utiliza un tipo de origen de datos que no admite las comprobaciones de conformidad, como las evidencias manuales, las llamadas a la API AWS o AWS CloudTrail.

Si la evidencia tiene un estado de verificación de conformidad que no es aplicable en la consola, se clasifica como no concluyente en el panel de control.

Pruebas conformes

La evidencia es conforme si una verificación de cumplimiento no informó de ningún problema. Este es el caso si Security Hub informa de un resultado de aprobación o AWS Config informa de un resultado de conformidad.

Dominios de control

El panel presenta el concepto de dominio de control. Piense en los dominios de control como una categoría general de controles que no es específica de ningún marco en particular. Las agrupaciones de dominios de control son una de las funciones más potentes del panel de control. Audit Manager destaca los controles de sus evaluaciones que contienen evidencias no conformes y los agrupa por dominio de control. Con esta característica, puede centrar sus esfuerzos de remediación en ámbitos temáticos específicos mientras se prepara para una auditoría.

> **Note**
>
> Tenga en cuenta que los dominios no son conjuntos de controles. Los conjuntos de controles son agrupaciones de controles específicas de un marco, que suelen definir los organismos reguladores. Por ejemplo, el marco PCI DSS tiene un conjunto de controles denominado “Requisito 8: identificar y autenticar el acceso a los componentes del sistema”. Este conjunto de control pertenece al dominio de control de la gestión de identidad y acceso.

Audit Manager clasifica los controles en los dominios de control siguientes.

Nombre de dominio de control	Descripción de lo que rigen los controles
Planificación de contingencia y continuidad del negocio	Cómo se establecen los procesos que protegen las operaciones comerciales críticas de los efectos de las principales interrupciones del sistema y la red.
Administración de cambios	Cómo se prueban, aprueban, implementan y documentan los cambios en su infraestructura de nube.

Nombre de dominio de control	Descripción de lo que rigen los controles
Seguridad y privacidad de datos	Cómo protege la privacidad, la disponibilidad y la integridad de sus datos.
Gestión del desarrollo y la configuración	Cómo se mantiene la infraestructura de la nube en el estado deseado y coherente.
Gobierno y supervisión	Cómo concuerda el uso de la computación en la nube con sus obligaciones legales, reglamentarias y éticas.
Administración de identidades y accesos	Cómo se asegura de que los usuarios correctos tengan el acceso adecuado a sus recursos tecnológicos.
Administración de incidentes	Cómo se establecen las responsabilidades y los procedimientos que garantizan una respuesta rápida y eficaz a los incidentes de seguridad.
Registro y monitoreo	Cómo se revisa la actividad de los usuarios para detectar indicios de que se ha intentado o realizado una actividad no autorizada.
Administración de red	Cómo se administra y opera la red de datos mediante un sistema de administración de red.
Administración de personal	Cómo se evalúan y gestionan los riesgos de seguridad del personal a nivel organizativo.
Seguridad física	Cómo se detectan y previenen los problemas de seguridad física en sus instalaciones.
Gestión de riesgos	Cómo se evalúan los posibles riesgos y pérdidas y cómo se reducen o eliminan dichas amenazas.
Gestión de la cadena de suministro	Cómo se identifican, evalúan y mitigan los riesgos asociados a los productos, proveedores y cadenas de suministro de TI.

Nombre de dominio de control	Descripción de lo que rigen los controles
Administración de los dispositivos de los usuarios	Cómo se reduce el riesgo de que el hardware de TI de sus empleados se pierda, se dañe o se esté en peligro.
Gestión de vulnerabilidades	Cómo se definen, evalúan y corrigen todas las vulnerabilidades conocidas de los activos de su infraestructura de nube.

Consistencia eventual de los datos

Los datos del panel de control son finalmente consistentes. Esto significa que, al leer datos del panel, podrían no reflejar de forma instantánea los resultados de una operación de escritura o actualización reciente. Si vuelve a comprobarlo al cabo de unas horas, el panel debería reflejar los datos más recientes.

Datos de evaluaciones eliminadas e inactivas

El panel muestra los datos de las evaluaciones activas. Si elimina una evaluación o cambia su estado a inactiva el mismo día que consulta el panel, los datos de esa evaluación se incluyen de la siguiente manera.

- Evaluaciones inactivas: si Audit Manager recopiló evidencia para su evaluación antes de cambiarla a inactiva, esos datos de evidencia se incluyen en los recuentos del panel de control para ese día.
- Evaluaciones eliminadas: si Audit Manager recopiló evidencia para su evaluación antes de eliminarla, esos datos de evidencia no se incluyen en los recuentos del panel de control para ese día.

Elementos del panel

En las siguientes secciones se describen los distintos componentes del panel.

Temas

- Controles con evidencia no conforme agrupados por dominio de control

Filtro de evaluación

Puede utilizar el filtro de evaluación para centrarse en una evaluación activa específica.

De forma predeterminada, el panel muestra los datos agregados de todas las evaluaciones activas. Si desea ver los datos de una evaluación específica, aplique un filtro de evaluación. Se trata de un filtro a nivel de página que se aplica a todos los widgets del panel de control.

Para aplicar el filtro de evaluación, seleccione una evaluación de la lista desplegable de la parte superior del panel. En esta lista se muestran hasta 10 de sus evaluaciones activas. Las evaluaciones creadas más recientemente aparecen primero. Si tiene muchas evaluaciones activas, puede empezar a escribir el nombre de una evaluación para encontrarla rápidamente. Después de seleccionar una evaluación, el panel muestra solo los datos de esa evaluación.

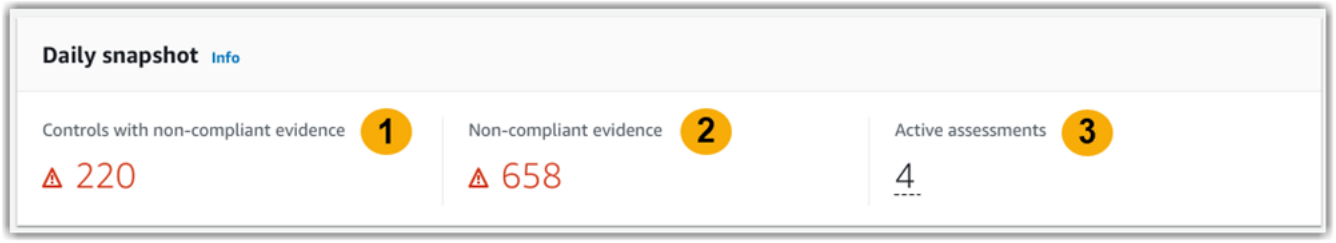
Instantánea diaria

Este widget muestra una instantánea del estado actual de cumplimiento de sus evaluaciones activas.

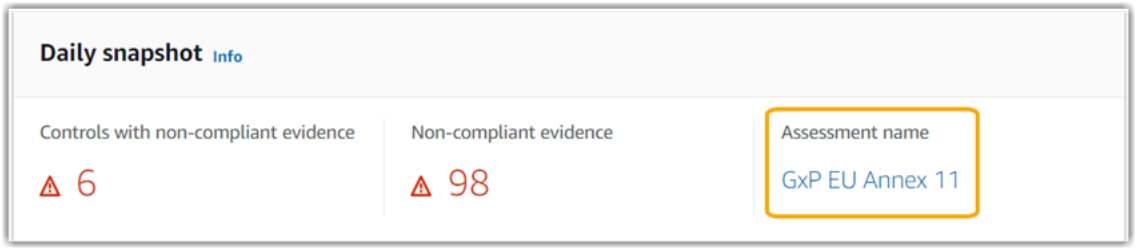
La instantánea diaria refleja los datos más recientes que se recopilaron en la fecha que aparece en la parte superior del panel. La fecha y la hora del panel de control se representan en la hora universal coordinada (UTC). Es importante entender que estos números son recuentos diarios basados en esta marca de tiempo. Hasta la fecha, no son una suma total.

De forma predeterminada, la instantánea diaria muestra los siguientes datos de todas las evaluaciones activas:

1. Controles con evidencias no conformes: el número total de controles asociados a evidencias no conformes.
2. Evidencia no conforme: cantidad total de evidencias de verificación de conformidad con una conclusión no conforme.
3. Evaluaciones activas: el número total de sus evaluaciones activas. Elija este número para ver los enlaces a estas evaluaciones.



Los datos de las instantáneas diarias cambian en función de los the section called “Filtro de evaluación” que aplique. Al especificar una evaluación, los datos reflejan únicamente los recuentos diarios de esa evaluación. En este caso, la instantánea diaria muestra el nombre de la evaluación que especificó. Puede elegir el nombre de la evaluación para abrirla.

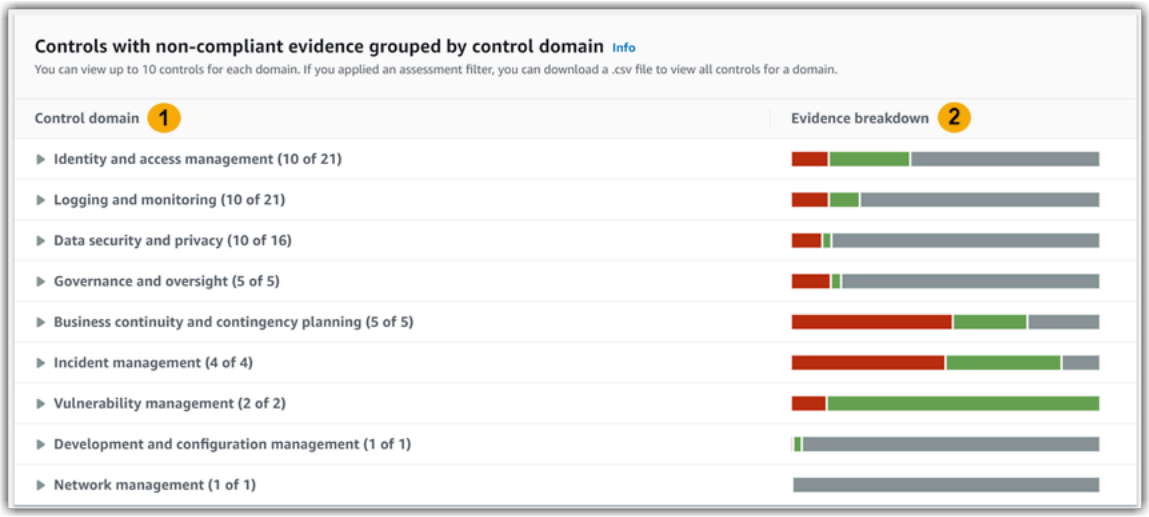


Controles con evidencia no conforme agrupados por dominio de control

Puede usar este widget para identificar qué controles tienen la mayor cantidad de evidencias no conformes.

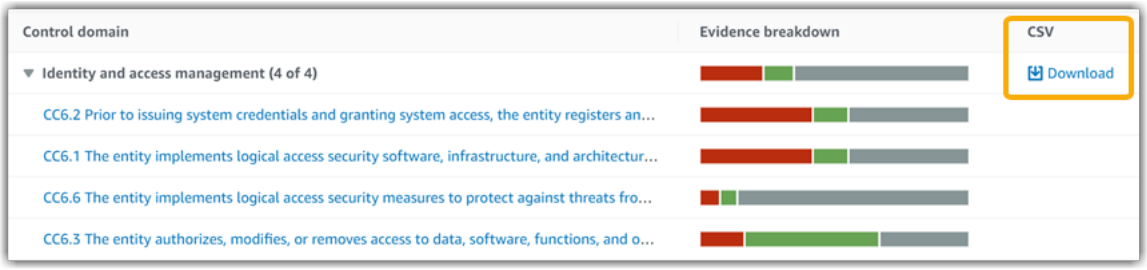
De forma predeterminada, el widget muestra los siguientes datos de todas las evaluaciones activas:

1. Dominio de control: una lista de los control domains que están asociados a sus evaluaciones activas.
2. Desglose de las evidencias: gráfico de barras que muestra un desglose del estado de cumplimiento de las evidencias.



Para expandir un dominio de control, elija la flecha situada junto a su nombre. Cuando se expande, la consola muestra hasta 10 controles para cada dominio. Estos controles se clasifican según el recuento total más alto de evidencias no conformes.

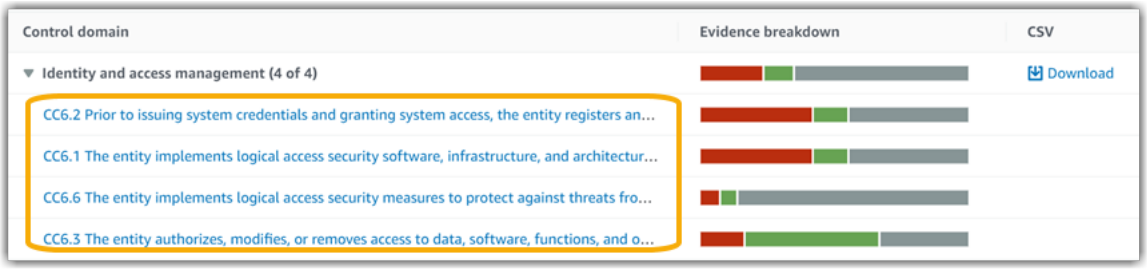
Los datos de este widget cambian en función de los the section called “Filtro de evaluación” que utilice. Cuando especifica una evaluación, solo ve los datos de esa evaluación. Además, también puede descargar un archivo .csv para cada dominio de control disponible en la evaluación.



El archivo .csv incluye la lista completa de los controles del dominio que están asociados a evidencias no conformes. En el siguiente ejemplo, se muestran las columnas de datos de .csv con valores ficticios.

	A	B	C	D	E	F	G
1	Date and Time	AssessmentID	AsessmentName	ControlId	ControlName	ControlDescription	DataSource
2	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	abcdefgh-1234-bcde-5678-cdefghijklmn	Control 1	Description of control 1	Manual
3	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	12345678-abcd-9012-bcde-345678901234	Control 2	Description of control 2	Manual
4	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	bcdefghi-2345-cdef-3456-defghijklmno	Control 3	Description of control 3	AWS Config, AWS Security Hub
5	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	23456789-bcde-0123-cdef-456789012345	Control 4	Description of control 4	Manual
6	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	cdefghij-3456-defg-4567-efghijklmnop	Control 5	Description of control 5	AWS Config
7	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	34567890-cdef-1234-defg-567890123456	Control 6	Description of control 6	Manual
8	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	defghijk-4567-efgh-5678-fghijklmnopq	Control 7	Description of control 7	AWS Config
9	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	45678901-defg-2345-efgh-678901234567	Control 8	Description of control 8	AWS Security Hub
10	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	efghijkl-5678-fghi-6789-ghijklmnopqr	Control 9	Description of control 9	Manual
11	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	56789012-efgh-3456-fghi-789012345678	Control 10	Description of control 10	Manual
12	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	fghijklm-6789-ghij-7890-hijklmnopqrs	Control 11	Description of control 11	Manual
13	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	67890123-fghi-4567-ghij-890123456789	Control 12	Description of control 12	Manual
14	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	ghijklmn-7890-hijk-8901-ijklmnopqrst	Control 13	Description of control 13	AWS Config, AWS Security Hub
15	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	78901234-ghij-5678-hijk-901234567890	Control 14	Description of control 14	Manual
16							

Por último, al aplicar un filtro de evaluación, los nombres de los controles de cada dominio aparecen con un hipervínculo. Elija cualquier control para abrir la página de detalles del control en la evaluación especificada.



> **Tip**
>
> Si utiliza la página de detalles del control como punto de partida, puede pasar de un nivel de detalle al siguiente.
>
> 1. Página de detalles del control: en esta página, la pestaña de carpetas de evidencias muestra las carpetas diarias de evidencias que Audit Manager recopiló para ese control. Para obtener más información, elija una carpeta.
> 2. Carpeta de evidencias: a continuación, puede revisar un resumen de la carpeta y una lista de las evidencias contenidas en esa carpeta. Para obtener más información, elija un elemento de evidencia individual.
> 3. Evidencia individual: por último, puede explorar los detalles de las evidencias individuales. Esto incluye todos los atributos y datos de recursos aplicables a la evidencia. Este es el nivel más detallado de datos de evidencia.

¿Qué tengo que hacer ahora?

Estos son algunos de los siguientes pasos que puede seguir después de revisar el panel.

- Descargar un archivo.csv: busque el dominio de evaluación y control en el que desee centrarse y descargue la lista completa de controles relacionados con evidencias que no cumplan con las normas.
- Revisar un control: después de identificar un control que necesite ser corregido, puede revisarlo.
- Delegar la revisión de un control: si necesita ayuda para revisar un control, puede delegar la revisión de un conjunto de controles.
- Editar su evaluación: si desea cambiar el alcance de una evaluación activa, puede editarla.

- Actualizar el estado de la evaluación: si desea dejar de recopilar evidencias para una evaluación, puede cambiar la evaluación a inactiva.

Solución de problemas

Para encontrar respuestas a preguntas y problemas habituales, consulte Solución de problemas del panel de control en la sección Solución de problemas de esta guía.

Evaluaciones en AWS Audit Manager

Las evaluaciones de Audit Manager se basan en marcos, es decir, en grupos de controles. Utilizando marcos como puntos de partida puede crear evaluaciones que recopilen evidencias sobre los controles de esos marcos. También puede definir el ámbito de las auditorías de sus evaluaciones. Esto incluye especificar para qué Cuentas de AWS y servicios desea recopilar evidencias.

Puede crear evaluaciones desde cualquier marco. Puede utilizar, o bien un marco estándar proporcionado por Audit Manager, o bien crear una evaluación a partir de un marco personalizado que cree usted mismo. Los marcos estándar contienen conjuntos de controles prediseñados que con arreglo a una norma o reglamento de cumplimiento específico. Los marcos personalizados, en cambio, contienen controles que puede personalizar y agrupar según sus requisitos de auditoría interna. Para más información sobre las diferencias entre los marcos estándar y los personalizados, consulte los marcos en el apartado Conceptos y terminología de esta guía.

Al crear una evaluación, se inicia la recopilación continua de evidencia. Llegado el momento de una auditoría, usted o un delegado pueden revisar estas evidencias y añadirlas a un informe de evaluación.

> **Note**
>
> AWS Audit Manager ayuda a recopilar evidencias relevantes para verificar el cumplimiento de normas y reglamentos de cumplimiento específicos. Sin embargo, no evalúa el cumplimiento en sí mismo. Por lo tanto, es posible que las evidencias recopiladas mediante AWS Audit Manager no incluyan toda la información sobre su uso de AWS que se necesita para las auditorías. AWS Audit Manager no sustituye a los asesores legales ni a los expertos en cumplimiento.

Temas

- Carga manual de evidencias en AWS Audit Manager
- Generación de informes de evaluación
- Cambio del estado de las evaluaciones a inactivas
- Eliminación de las evaluaciones

Creación de las evaluaciones

Este tema se basa en el tutorial Primeros pasos: creación de una evaluación. Contiene instrucciones detalladas sobre cómo crear una evaluación a partir de un marco. Siga estos pasos para crear una evaluación e iniciar la recopilación continua de evidencia.

Tareas

- Paso 1: especificar los detalles de la evaluación
- Paso 2: especificar las Cuentas de AWS que se incluyen en la evaluación
- Paso 3: especificar las Servicios de AWS objeto de evaluación
- Paso 4: Especificar los responsables de la auditoría
- Paso 5: Revisar y crear
- ¿Cuál es el siguiente paso?

Paso 1: especificar los detalles de la evaluación

Comience seleccionando un marco y proporcione la información básica necesaria para su evaluación.

Pasos para especificar los detalles de la evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Evaluación y, a continuación, elija Crear evaluación.
   - Otra opción es elegir Introducción en el panel de control y, a continuación, Crear evaluación.
3. Escriba el nombre de su evaluación en Nombre de la evaluación.
4. (Opcional) Agregue una descripción de su evaluación en Descripción de la evaluación.
5. En Destino de los informes de evaluación, elija el bucket de Amazon S3 existente en el que desee guardar los informes de evaluación.

> **Tip**
>
> El destino predeterminado del informe de evaluación depende de la configuración de Audit Manager. Para más información, consulte Configuración de AWS Audit Manager y destino de los informes de evaluación. Si lo prefiere, puede crear y usar varios grupos de S3 para organizar sus informes de evaluación.

6. En Marcos, seleccione el marco a partir del cual desea crear la evaluación. También puede buscar en la barra de búsqueda para encontrar un marco por su nombre o por una norma o reglamento de cumplimiento.

> **Tip**
>
> Para más información sobre un marco, elija el nombre del marco en cuestión. Se abrirá la página de resumen del marco, donde puede revisar el contenido del mismo. Esto incluye los controles y los orígenes de datos del marco.

7. En Etiquetas, elija Agregar nueva etiqueta para asociar una etiqueta a su evaluación. Puede especificar una clave y un valor para cada etiqueta. La clave de etiqueta es obligatoria; podrá utilizarla como criterio de búsqueda para esta evaluación. Para más información acerca del uso de etiquetas en Audit Manager, consulte Etiquetado de recursos de AWS Audit Manager.
8. Elija Siguiente.

> **Note**
>
> Es importante que se asegure de que la evaluación recopile las evidencias correctas para un marco determinado. Antes de comenzar con la recopilación de evidencias, le recomendamos que revise los requisitos del marco elegido. A continuación, valídelos los parámetros actuales de la regla de AWS Config. Para garantizar que estos parámetros se ajustan a los requisitos del marco, puede actualizar la regla en AWS Config.
> Supongamos, por ejemplo, que está creando una evaluación para CIS v1.2.0. Este marco tiene un control denominado 1.9: asegúrese de que la política de contraseñas de IAM exija una longitud mínima de 14 o más. En AWS Config, la regla política de contraseñas de IAM tiene un parámetro `MinimumPasswordLength` que comprueba la longitud de la contraseña. El valor predeterminado para este parámetro es 14 caracteres. Por lo tanto, la regla concuerda con los requisitos de control establecidos. Si no utiliza el valor de parámetro

predeterminado, asegúrese de que sea igual o superior al requisito de 14 caracteres establecido en CIS v1.2.0. Encontrará información relativa a los parámetros predeterminados de cada regla administrada en la documentación de AWS Config.

Paso 2: especificar las Cuentas de AWS que se incluyen en la evaluación

Puede especificar varias Cuentas de AWS que sean objeto de evaluación. Audit Manager admite varias cuentas gracias a la integración con AWS Organizations. Esto significa que las evaluaciones de Audit Manager se pueden ejecutar en varias cuentas, de modo que las evidencias recopiladas se consolidan en una cuenta del administrador delegado. Para activar las organizaciones en Audit Manager, consulte Habilitar AWS Organizations (opcional).

> **Note**
>
> Audit Manager admite aproximadamente hasta 150 cuentas de miembros por evaluación. Si intenta incluir más de 150 cuentas, es posible que no se pueda crear la evaluación.

Pasos para especificar Cuentas de AWS objeto de evaluación

1. En Cuentas de AWS, seleccione las Cuentas de AWS que desee evaluar.
   - Si ha activado las organizaciones en Audit Manager, se mostrarán varias cuentas. Puede elegir una o más cuentas de la lista. Alternativamente también puede buscar una cuenta por el nombre de la cuenta, el ID o el correo electrónico.
   - Si no activó las organizaciones en Audit Manager, solo aparecerá su Cuenta de AWS actual.
2. Elija Siguiente.

> **Note**
>
> Cuando se elimina una cuenta incluida de su organización, Audit Manager deja de recopilar evidencias de esa cuenta. No obstante, la cuenta sigue apareciendo en la pestaña de Cuentas de AWS de su evaluación. Para eliminar la cuenta de la lista de cuentas incluidas, puede editar la evaluación. Las cuentas eliminadas no aparecen en la lista durante la edición y podrá guardar los cambios sin ellas.

Paso 3: especificar las Servicios de AWS objeto de evaluación

El marco que seleccionó anteriormente define los Servicios de AWS que Audit Manager monitorea y para los que recopila evidencia. Si un Servicio de AWS de la lista no está seleccionado, o si lo está pero no lo habilitó en su entorno, Audit Manager no recopilará evidencias de los recursos relacionados con dicho servicio.

Puede especificar los Servicios de AWS que se deban incluir en la evaluación de la siguiente manera.

Pasos para las evaluaciones creadas a partir de marcos estándar

Al utilizar la consola de Audit Manager para crear evaluaciones a partir de un marco estándar, la lista de dentro de Servicios de AWS objeto de evaluación se selecciona de forma predeterminada. Esta lista no se puede editar Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. La selección se realiza de acuerdo con los requisitos del marco estándar. Si el marco estándar que ha seleccionado contiene solo controles manuales, ningún Servicios de AWS está incluido en su evaluación y no podrá añadir ningún servicio a su evaluación.

Para continuar, compruebe la lista y elija Siguiente.

> **Tip**
>
> Si necesita editar la lista de servicios incluidos, puede hacerlo mediante la API Crear evaluación de Audit Manager.
> También puede personalizar el marco estándar y, a continuación, crear una evaluación a partir de dicho marco.

Pasos para las evaluaciones creadas a partir de marcos personalizados

Si seleccionó un marco personalizado en el paso 1, puede revisar y modificar la lista de los Servicios de AWS que están incluidos en su evaluación. Si el marco personalizado que ha seleccionado contiene solo controles manuales, se muestran todos los Servicios de AWS pero no se selecciona ninguno. Puede no seleccionar ningún servicio o elegir varios para incluirlos en su evaluación.

Pasos para especificar qué Servicios de AWS se evalúan (solo para las evaluaciones creadas a partir de marcos personalizados)

1. En Servicios de AWS, seleccione los servicios que desee incluir en la evaluación. Para encontrar servicios adicionales, utilice la barra de búsqueda para buscar por servicio, categoría o descripción. Para agregar un servicio, active la casilla de verificación situada junto al nombre del servicio. Para eliminar un servicio, desactive la casilla de verificación.
2. Cuando ya haya seleccionado todos los Servicios de AWS que desee, elija Siguiente.

Paso 4: Especificar los responsables de la auditoría

En este paso, especifique quiénes son los responsables de la auditoría en la evaluación. Los responsables de la auditoría son las personas de su empresa u organización (normalmente de los equipos de GRC, SecOps o DevOps) que se encargan de gestionar la evaluación de Audit Manager. Se recomienda que utilicen la política AWSAuditManagerAdministratorAccess.

Pasos para especificar los responsables de la auditoría

1. En Responsables de la auditoría, revise la lista actual de las personas encargadas de las auditorías. La columna de responsables de las auditorías muestra sus ID de usuario y los roles correspondientes. La columna de Cuenta de AWS muestra los Cuenta de AWS asociados a dicho responsable de auditoría.
2. Los responsables de auditoría que tienen una casilla de verificación activada son los que se incluyen en la evaluación. Desactive la casilla de verificación de los responsables de auditoría que desee eliminar de la evaluación. Para encontrar otros responsables de auditoría, utilice la barra de búsqueda para buscar por nombre o Cuenta de AWS.
3. Cuando haya terminado, elija Siguiente.

Paso 5: Revisar y crear

Revise de la información de su evaluación. Para modificar la información de un paso, seleccione Editar. Cuando haya terminado, elija Crear evaluación.

Esta acción inicia la recopilación continua de evidencias para su evaluación. Tras crear una evaluación, la recopilación de evidencias continúa hasta que el estado de la evaluación cambia a inactiva. También puede detener la recopilación de evidencias para un control específico cambiando el estado del control a inactivo.

> **Note**
>
> Las evidencias automatizadas estarán disponibles 24 horas después de que se haya creado la evaluación. Audit Manager recopila automáticamente evidencias de varios orígenes de datos, y la frecuencia con la que lo hace depende del tipo de evidencia. Para más información, consulte Frecuencia de recolección de evidencias en esta guía.

¿Cuál es el siguiente paso?

Una vez creada la evaluación, puede obtener más información acerca de varios temas:

- Acceso a las evaluaciones
- Revisión de las evaluaciones
- Edición de las evaluaciones
- Revisión de los controles de una evaluación
- Revisión de las evidencias de una evaluación
- Carga manual de evidencias a las evaluaciones
- Delegación en AWS Audit Manager
- Generación de informes de evaluación
- Cambio de estado de las evaluaciones
- Eliminación de las evaluaciones
- Solución de problemas de evaluación y recopilación de pruebas

Acceso a las evaluaciones en AWS Audit Manager

Puede ver todas sus evaluaciones en la página Evaluaciones de la consola de Audit Manager. Desde aquí, también puede editar una evaluación, eliminarla o crear una evaluación nueva.

También puede ver sus evaluaciones mediante la API de Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

Pasos para ver sus evaluaciones (en la consola)

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija Evaluaciones para ver una lista de las evaluaciones activas y pasadas. También puede utilizar la barra de búsqueda para buscar una evaluación en concreto.
3. Elija el nombre de una evaluación para abrir una página de resumen en la que podrá ver los detalles de dicha evaluación.

AWS CLI

Pasos para ver sus evaluaciones (en CLI)

Para ver las evaluaciones en Audit Manager, ejecute el comando list-assessments. Puede utilizar el subcomando `--status` para ver las evaluaciones activas o inactivas.

```
aws auditmanager list-assessments --status ACTIVE
```

```
aws auditmanager list-assessments --status INACTIVE
```

Audit Manager API

Pasos para ver sus evaluaciones (en la API)

Para ver las evaluaciones en Audit Manager, utilice la operación ListAssessments. Puede utilizar el atributo de estado para ver las evaluaciones activas o inactivas.

Para más información, consulte uno de los enlaces anteriores de la referencia de la API de AWS Audit Manager. Encontrará, entre otros, una explicación sobre cómo utilizar la operación de `ListAssessments` y los parámetros en uno de los SDK específicos del lenguaje de AWS.

Edición de las evaluaciones

Puede editar sus evaluaciones activas en Audit Manager y modificar cambiar información como la descripción, el ámbito de evaluación, los responsables de la auditoría y el destino del informe de evaluación.

Tareas

- Paso 1: editar los detalles de la evaluación
- Paso 2: editar las Cuentas de AWS que se van a evaluar
- Paso 3: editar los Servicios de AWS objeto de evaluación
- Paso 4: edite los responsables de la auditoría
- Paso 5: revisar y crear

Paso 1: editar los detalles de la evaluación

Siga estos pasos para editar los detalles de su evaluación.

Pasos para editar una evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Evaluaciones para ver su lista actual de evaluaciones.
3. Seleccione una evaluación y elija Editar.
   - También puede abrir la evaluación y, a continuación, seleccionar Editar en la parte superior derecha de la página.
4. En Editar los detalles de la evaluación, modifique el nombre, la descripción y el destino del informe de evaluación.
5. Elija Siguiente.

> **Tip**
>
> Para modificar las etiquetas de una evaluación, abra la evaluación y elija Pestaña de etiquetas. Aquí puede ver y editar las etiquetas asociadas a la evaluación.

Paso 2: editar las Cuentas de AWS que se van a evaluar

En este paso, puede cambiar la lista de cuentas incluidas en la evaluación.

Audit Manager admite varias cuentas gracias a la integración con AWS Organizations. En consecuencia, las evaluaciones de Audit Manager pueden ejecutarse en varias cuentas, y las

evidencias recopiladas se consolidan en la cuenta del administrador o administradores delegados. Para añadir o cambiar un administrador delegado para Audit Manager, consulte AWS Audit ManagerConfiguración de administradores delegados.

> **Note**
>
> Audit Manager admite aproximadamente hasta 150 cuentas de miembros por evaluación. Si intenta incluir más de 150 cuentas, es posible que no se pueda crear la evaluación.

Pasos para editar Cuentas de AWS incluidas en la evaluación

1. En Editar Cuentas de AWS objeto de evaluación, seleccione las cuentas AWS adicionales aplicables. También puede eliminar cuentas quitándolas de la lista.
2. Elija Siguiente.

Paso 3: editar los Servicios de AWS objeto de evaluación

En este paso se especifica qué Servicios de AWS monitorea Audit Manager y de cuáles recopila evidencias. Si un Servicio de AWS que aparece en la lista no está seleccionado, o si lo está seleccionada pero no se habilitó en su entorno, Audit Manager no recopilará evidencias de los recursos relacionados con el servicio.

Puede revisar y editar los Servicios de AWS que se incluyen en la evaluación de la siguiente manera.

Pasos para las evaluaciones creadas a partir de marcos estándar

Cuando utiliza la consola de Audit Manager para editar una evaluación creada a partir de un marco estándar, puede revisar la lista de Servicios de AWS incluidos en la evaluación, pero no puede editarla. Esto se debe a que Audit Manager asigna y selecciona automáticamente los orígenes de datos y los servicios en su lugar según el diseño del marco estándar. Si la evaluación se creó utilizando un marco que solo contiene controles manuales, no se incluye ningún Servicios de AWS para evaluar ni se puede añadir ninguno.

Para continuar, compruebe la lista y elija Siguiente.

> **Tip**
>
> Si necesita editar la lista de servicios que se incluyen en la evaluación existente, puede hacerlo utilizando la API Actualizar evaluación que proporciona Audit Manager.

Pasos para las evaluaciones creadas a partir de marcos personalizados

Si la evaluación se ha creado a partir de un marco personalizado, puede editar los Servicios de AWS que se van a evaluar. Puede no seleccionar ningún servicio o elegir varios para incluirlos en su evaluación.

Pasos para editar los Servicios de AWS objeto de evaluación (solo para las evaluaciones creadas a partir de marcos personalizados)

1. En Editar Servicios de AWSobjeto de evaluación, seleccione los Servicios de AWS adicionales aplicables. También puede eliminar servicios quitándolos de la lista.
2. Elija Siguiente.

Paso 4: edite los responsables de la auditoría

También puede cambiar los responsables de auditoría para su evaluación. Los responsables de la auditoría son las personas de su empresa u organización (normalmente de los equipos de GRC, SecOps o DevOps) que se encargan de gestionar la evaluación de Audit Manager. Se encargan, entre otros, de delegar los conjuntos de controles para su revisión y de generar informes de evaluación. Le recomendamos que utilice la política AWSAuditManagerAdministratorAccess.

Pasos para editar los responsables de las auditorías

1. Seleccione los nuevos responsables de la auditoría y agréguelos a su evaluación. Para eliminar a los responsables de auditoría, quítelos de la lista.
2. Elija Siguiente.

Paso 5: revisar y crear

Revise de la información de su evaluación. Para modificar la información de un paso, seleccione Editar. Cuando haya terminado de editar, elija Guardar cambios para confirmarlos.

> **Note**
>
> Tras completar las modificaciones, los cambios en la evaluación entrarán en vigor a las 00:00 UTC del día siguiente.

Revisión de las evaluaciones

Tras crear las evaluaciones en Audit Manager, puede abrirlas y revisarlas en cualquier momento.

Pasos para abrir y revisar una evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija Evaluaciones y verá una lista de sus evaluaciones.
3. Seleccione el nombre de la evaluación que desee consultar y ábrala.

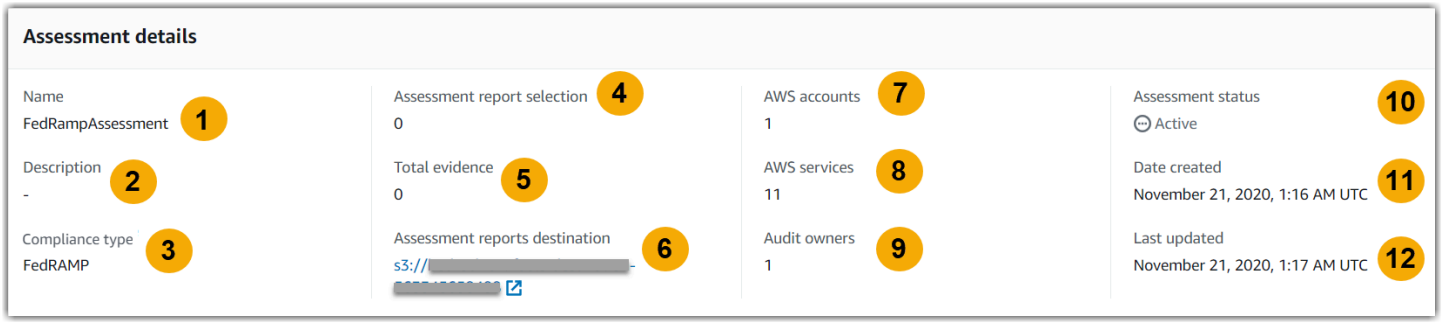
Al abrir una evaluación, verá una página de resumen que contiene varios apartados. Las secciones de esta página y su contenido se describen a continuación.

Secciones de las páginas de evaluación

- Detalles de las evaluaciones
- Pestaña de controles
- Pestaña de selección del informe de evaluación
- Pestaña Cuentas de AWS
- Pestaña Servicios de AWS
- Pestaña de responsables de la auditoría
- Pestaña de etiquetas
- Pestaña del registro de cambios

Detalles de las evaluaciones

El apartado de detalles de la evaluación proporciona una visión general de la evaluación.



Contiene la información siguiente:

1. Nombre: el nombre que se introdujo para la evaluación.
2. Descripción: la descripción opcional que se agregó a la evaluación.
3. Tipo de conformidad: norma o reglamento de conformidad en el que se basa la evaluación.
4. Selección del informe de evaluación, que determina el número de evidencias que se incluirán en el informe de evaluación.
5. Total de evidencias, que indica el número total de elementos probatorios que se recopilan para la evaluación.
6. Destino de los informes de evaluación, es decir, el bucket de Amazon S3 en el que Audit Manager guarda el informe de evaluación.
7. Cuentas de AWS: el número de Cuentas de AWS que se incluyen en la evaluación.
8. Servicios de AWS: el número de Servicios de AWS que se incluyen en la evaluación.
9. Responsables de la auditoría, que define el número de responsables de la auditoría para la evaluación.
10. Estado de la evaluación, es decir, el estadío en el que se encuentra la evaluación.
    - Activo: indica que la evaluación está recopilando evidencias en este momento. Las evaluaciones recién creadas tienen este estado.
    - Inactiva: indica que la evaluación ya no recopila evidencias. Para más información sobre los informes de evaluación, consulte Cambio del estado de las evaluaciones a inactivas.
11. Fecha de creación, es decir el día en que se creó la evaluación.
12. Última actualización, es decir la fecha más reciente en la que se editó esta evaluación.

Pestaña de controles

La pestaña Controles contiene un resumen de los controles de la evaluación, así como una lista completa de dichos controles. Cada evaluación puede contener varios conjuntos de controles; a su vez, cada conjunto de controles contiene varios controles. Los controles y los conjuntos de controles se organizan de manera que coincidan con el diseño definido en la norma o reglamento de cumplimiento correspondientes.

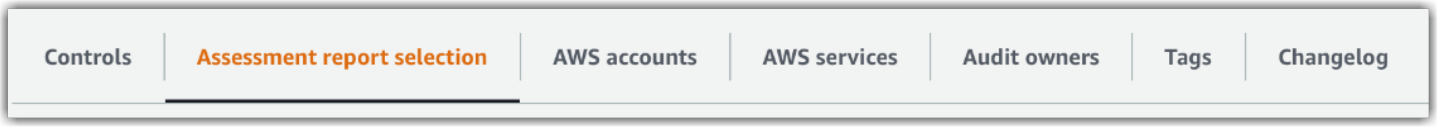
El resumen del estado del control proporciona un resumen de los controles para la evaluación. En concreto, la tabla resumen incluye la información siguiente:

- Controles totales hace referencia al número total de controles de la evaluación.
- Revisado: el número de controles que revisó la persona responsable o delegada de la auditoría.
- Revisión en curso: el número de controles que se está revisando actualmente.
- Inactivo: el número de controles que ya no recopilan evidencias de forma activa.

En la tabla conjuntos de controles, se muestra una lista de controles agrupados por conjuntos de controles. Puede expandir o contraer los controles de cada conjunto. Si le interesa un control en concreto, también puede buscar por nombre de control. Las columnas de datos siguientes aparecen en la tabla Controles agrupados por conjuntos de controles:

- Controles agrupados por conjuntos de controles hace referencia al nombre del conjunto de control.
- Estado del control, es decir, el estadío en el que se encuentra el estado del control.
  - En revisión indica que este control aún no se ha revisado. Todavía se están recopilando evidencias para este control y puede cargarlas manualmente. Este es el valor predeterminado.
  - Revisado indica que ya se revisaron las evidencias de este control. No obstante, se siguen recopilando evidencias y puede cargarlas manualmente.
  - El estado inactivo, indica que la recopilación automática de evidencias se ha interrumpido para este control. Ya no puede cargar evidencias manuales.
- Delegado a indica el revisor de este control, si se asignó a un delegado para su revisión.
- Total de evidencias, es decir el número de evidencias que se ha recopilado para este control.

Pestaña de selección del informe de evaluación



Esta pestaña detalla la lista de evidencias que se deben incluir en el informe de evaluación, agrupadas por carpetas de evidencia. Estas carpetas de evidencias se organizan y nombran en función de la fecha en que se crearon. Puede examinar estas carpetas y seleccionar qué evidencias desea incluir en su informe de evaluación. También puede utilizar la barra de búsqueda para buscar por nombre de carpeta de evidencias o nombre de control. El número total de evidencias que se añade al informe de evaluación se resume en el apartado de detalles de la evaluación, que encontrará en la parte superior de la página.

La tabla de selección del informe de evaluación muestra una lista de carpetas de evidencias con los siguientes datos:

- Carpetas de evidencias, es la denominación de la carpeta o carpetas de evidencias. El nombre de la carpeta se basa en la fecha en que se recopiló la evidencia.
- Evidencias seleccionadas, es decir el número de evidencias de la carpeta que se incluye en el informe de evaluación.
- Nombre del control, es decir el nombre del control asociado a esta carpeta de evidencia.

Para más información sobre cómo añadir evidencias a un informe de evaluación, consulte Generación de informes de evaluación.

Pestaña Cuentas de AWS

Esta pestaña muestra la lista de las Cuentas de AWS que se incluyen en la evaluación. El número total de cuentas se resume en el apartado de detalles de la evaluación, que aparece en la parte superior de la página.

La tabla de Cuentas de AWS presenta una lista de cuentas con los datos siguientes:

- ID de la cuenta, es decir la identificación de la cuenta de Cuenta de AWS.

- Nombre de la cuenta, es decir la denominación que recibe la Cuenta de AWS.
- Correo electrónico, es decir la dirección de correo electrónico asociada a la Cuenta de AWS.

Pestaña Servicios de AWS

Esta pestaña muestra la lista de los Servicios de AWS que se incluyen en la evaluación. En otras palabras, estos son los Servicios de AWS sobre los cuales su evaluación recopila evidencias.

El número total de servicios se resume el apartado de detalles de la evaluación, que encontrará en la parte superior de la página.

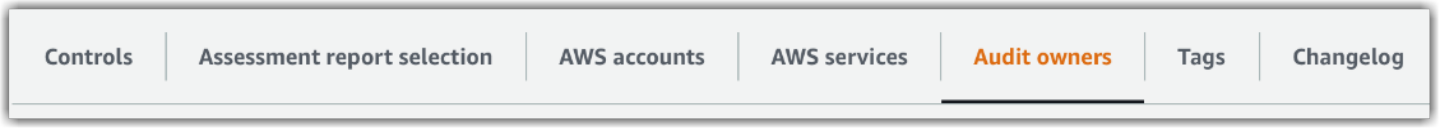
La tabla de Servicios de AWS muestra una lista de servicios con los datos siguientes:

- Servicio de AWS: nombre del Servicio de AWS.
- Categoría: la categoría de servicio, por ejemplo cálculo o base de datos.

Audit Manager realiza evaluaciones de recursos para los servicios que se detallan en la tabla. Por ejemplo, si Amazon S3 aparece en la lista, Audit Manager puede recopilar evidencias sobre sus buckets de S3. Las evidencias exactas que se recopilan dependen del origen de los datos del control. Por ejemplo, si el tipo de fuente de datos es AWS Config, y la asignación del origen de datos es una regla de AWS Config (como `s3-bucket-public-write-prohibited`), Audit Manager recopilará el resultado de la evaluación de esa regla como evidencia. Para más información, consulte ¿Cuál es la diferencia entre un servicio incluido y un tipo de origen de datos? en esta guía.

> **Note**
>
> Si su evaluación se creó en la consola a partir de un marco estándar, Audit Manager seleccionó los servicios por usted y asignó sus orígenes de datos de acuerdo con los requisitos del marco. Si el marco estándar solo contiene controles manuales, no habrá ningún Servicios de AWS objeto de análisis. Si necesita editar la lista de servicios que se van a analizar, puede utilizar la API UpdateAssessment.

Pestaña de responsables de la auditoría

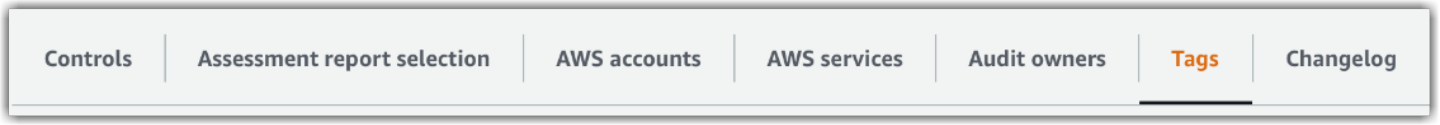


En esta pestaña se detallan los responsables de la auditoría de la evaluación. El número total de responsables de la auditoría también se resume en el apartado de detalles de la evaluación, que encontrará en la parte superior de la página.

La tabla de responsables de la auditoría muestra una lista de las cuentas con los siguientes datos:

- Responsable de la auditoría: nombre de la persona responsable de la auditoría.
- Cuenta de AWS: dirección de correo electrónico asociada con la persona responsable.

Pestaña de etiquetas



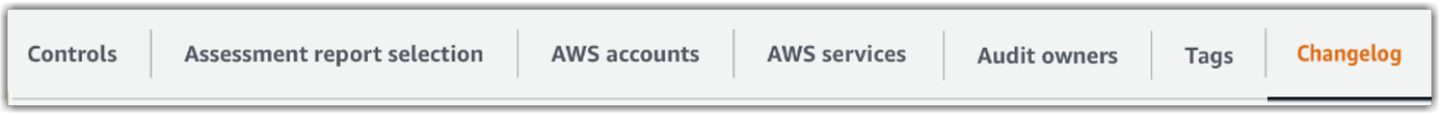
Esta pestaña presenta una lista de etiquetas heredadas del marco que se utilizan para crear esta evaluación. El número total de etiquetas se resume en Detalle de la evaluación, que aparece en la parte superior de la página.

La tabla de Etiquetas muestra una lista de servicios con los datos siguientes:

- Claves se refiere a la clave de la etiqueta; por ejemplo un estándar de conformidad, un reglamento o una categoría.
- Valor especifica el valor de la etiqueta.

Para más información acerca del uso de etiquetas en Audit Manager, consulte Etiquetado de recursos de AWS Audit Manager.

Pestaña del registro de cambios



Esta pestaña incluye una lista de la actividad de los usuarios relacionada con la evaluación.

La tabla registro de cambios incluye una lista de cuentas con los siguientes datos:

- Fecha, es decir el día en que se produjo la actividad.
- Usuario. es decir quién realizó la acción.
- Acción detalla la acción que se produjo, por ejemplo la creación de una evaluación.
- Tipo especifica el tipo de objeto que ha cambiado, por ejemplo una evaluación.
- Recurso, es decir, el recurso que se vio afectado por el cambio, como el marco a partir del cual se creó la evaluación.

Revisión de los controles de una evaluación

Los controles de Audit Manager le ayudan a cumplir con los estándares y reglamentos de conformidad comunes y específicos de sus auditorías. Puede abrir y revisar los controles de su evaluación de Audit Manager en cualquier momento.

Pasos para abrir una página de resumen de controles

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Evaluaciones y, a continuación, el nombre de una evaluación y ábrala.
3. En la página de evaluación, seleccione la pestaña Controles, desplácese hacia abajo hasta llegar a la tabla conjuntos de controles y, a continuación, elija el nombre del control que desea abrir.

Al abrir un control, verá una página de resumen que contiene varias secciones. Las secciones de esta página y su contenido se describen en los apartados que siguen.

Secciones de la página de control

- Detalles de control
- Actualización del estado de control
- Pestaña de carpetas de evidencias
- Tipos de origen de datos
- Pestaña de comentarios
- Pestaña del registro de cambios

Detalles de control

El apartado Detalles del control ofrece una visión general del control.

Contiene la información siguiente:

1. Nombre del control: el nombre que recibe dicho control.
2. Descripción del control, es decir, la descripción proporcionada para el control.
3. Información de evaluación, donde se detallan los procedimientos de prueba recomendados para el control.
4. Plan de acción, es decir las acciones recomendadas en caso de que el control no se complete con éxito.

Actualización del estado de control

Puede revisar y actualizar el estado del control de evaluación en el apartado Actualización del estado del control.

Los siguientes estados están disponibles:

- En revisión: indica que este control aún no se ha revisado. Todavía se están recopilando evidencias para este control y puede cargarlas manualmente. Este es el valor predeterminado.
- Revisado indica que se han revisado las evidencias de este control. No obstante, se siguen recopilando evidencias y puede cargarlas manualmente.
- El estado inactivo, indica que la recopilación automática de evidencias se ha interrumpido para este control. Ya no puede cargar evidencias manuales.

> **Note**
>
> El cambio de un estado de control a revisado es definitivo. Tras establecer el estado de un control como revisado, ya no podrá cambiar el estado de ese control ni volver a un estado anterior.

Pestaña de carpetas de evidencias

La pestaña Carpetas de evidencias muestra las evidencias que se recopila automáticamente para este control. Se organizan en carpetas a diario.

La tabla de carpetas de evidencias muestra una lista de carpetas con los siguientes datos:

- Carpetas de evidencias, es la denominación de la carpeta o carpetas de evidencias. El nombre se basa en la fecha en que se recopiló o agregó manualmente la evidencia o evidencias.
- Comprobación de conformidad, es decir el número de problemas que se encuentran en la carpeta o carpetas de evidencias. Representa el número total de problemas de seguridad que se notificaron directamente de AWS Security Hub, AWS Config o de ambos. Puede aparecer la opción No aplicable. Esto indica que, o bien no tiene AWS Security Hub o AWS Config habilitadas, o bien las evidencias provienen de un tipo de origen de datos diferente.
- Total de evidencias, es decir el número de evidencias incluidas en la carpeta.
- Selección del informe de evaluación, es decir el número de evidencias de la carpeta que se incluyen en el informe de evaluación.

En la pestaña Carpetas de evidencias puede realizar las acciones siguientes:

- Revisar las evidencias una a una. Para ello, elija primero una carpeta de evidencias y ábrala. En la página de resumen de la carpeta de evidencias, puede elegir qué evidencia desea revisar.
- Agregar evidencias manuales: para más información, consulte Carga manual de evidencias en AWS Audit Manager.
- Añadir evidencias a un informe de evaluación: para más información, consulte Generación de informes de evaluación.

Tipos de origen de datos

Esta pestaña muestra información acerca de los orígenes de datos para el control. Contiene la información siguiente:

- Nombre del origen de datos, que se aplica únicamente a los controles personalizados. Hace referencia al nombre descriptivo que ha asignado a cada origen de datos. Puede usarlo para distinguir entre varios orígenes de datos que pertenecen al mismo tipo de origen de datos.
- Tipo de origen de datos, que especifica de dónde provienen los datos de evidencia.

  - Si Audit Manager recopila evidencias, el origen de datos puede ser de cuatro tipos: AWS Security Hub, AWS ConfigAWS CloudTrail, o llamadas a la API de AWS.
  - Si carga sus propias evidencias, el tipo de origen de datos es Manual. Las descripciones indican si la evidencia manual requerida es una carga de archivos o una respuesta de texto.
- El atributo de asignación se usa para identificar y recuperar datos del origen de datos.
  - Si el tipo de origen de datos es AWS Config, la asignación será el nombre de una regla de AWS Config en concreto (por ejemplo, `EC2_INSTANCE_MANAGED_BY_SSM`). Audit Manager utiliza esta asignación para informar del resultado de esa verificación de reglas directamente desde AWS Config.
  - Si el tipo de origen de datos es AWS Security Hub, la asignación es el nombre de una regla específica (por ejemplo, `1.1 – Avoid the use of the "root" account`). Audit Manager utiliza esta asignación para informar del resultado del control de seguridad directamente desde Security Hub.
  - Si el tipo de origen de datos es AWS, la asignación es el nombre de llamada a la API específica (por ejemplo, `ec2_DescribeSecurityGroups`). Audit Manager utiliza esta asignación para recopilar la respuesta de la API.
  - Si el tipo de origen de datos es AWS CloudTrail, la asignación es el nombre de un evento de CloudTrail específico (por ejemplo, `CreateAccessKey`). Audit Manager utiliza esta asignación para recopilar la actividad relacionada de los usuarios de sus registros de CloudTrail.
- Frecuencia se refiere a la asiduidad con la que se recopila evidencias a partir de este origen de datos y varía en función del origen de datos. Para más información, elija el valor de la columna o consulte Frecuencia de recolección de evidencias.

Pestaña de comentarios

En la pestaña Comentarios, puede añadir información sobre el control y sus evidencias. También muestra una lista de los comentarios anteriores.

En Enviar comentarios, puede escribir comentarios de texto para un control y enviarlos con Enviar comentarios.

En Comentarios anteriores verá una lista de los comentarios anteriores junto con la fecha en la que se agregaron y el ID del usuario que los introdujo.

Pestaña del registro de cambios

La pestaña Registro de cambios muestra una lista de la actividad de los usuarios relacionada con el control. La misma información está disponible como registros de auditoría en AWS CloudTrail. Con la actividad del usuario que se captura directamente en Audit Manager, puede revisar fácilmente los registros de auditoría de la actividad de un control determinado.

La tabla del registro de cambios incluye las columnas de datos siguientes:

- Fecha muestra la fecha y hora de la actividad, representadas en tiempo universal coordinado (UTC).
- Usuario hace referencia al usuario o rol que realizó la actividad.
- Acción incluye una descripción de la actividad.
- Tipo es el atributo asociado que describe con más detalle la actividad.
- Recurso, es decir el recurso relacionado con la actividad, si corresponde.

Audit Manager rastrea la actividad siguiente de los usuarios en los registros de cambios:

- Creación de las evaluaciones
- Edición de las evaluaciones
- Compleción de las evaluaciones
- Eliminación de las evaluaciones
- Delegación de conjuntos de controles para su revisión
- Envío de conjuntos de controles revisados a la persona responsable de la auditoría
- Carga de evidencias manual
- Actualización del estado de los controles
- Generación de informes de evaluación

Revisión de las evidencias de una evaluación

Las evaluaciones activas en Audit Manager recopilan evidencias de varios orígenes de datos de forma automática. Para obtener más información, consulte ¿Cómo recopila AWS Audit Manager las evidencias?. Puede abrir y revisar las evidencias de los controles de sus evaluaciones en cualquier momento.

Pasos para abrir evidencias para un control

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Evaluaciones y, a continuación, el nombre de la evaluación que desee abrir.
3. En la página de evaluación, seleccione la pestaña Controles: desplácese hacia abajo hasta llegar a la tabla Controles y, a continuación, elija el nombre del control que desee abrir.
4. En la página de control, seleccione la pestaña Carpetas de evidencias. En la tabla de carpetas de evidencias se muestra una lista de todas las carpetas de evidencias del control. Las carpetas se organizan y nombran en función de la fecha en que se recopiló las evidencias que contiene la carpeta.
5. Elija el nombre de una carpeta de evidencias para abrirla.

Puede revisar la carpeta de evidencias para el control desde aquí mismo y profundizar para revisar las evidencias una a una según sea necesario.

Temas

- Revisión de las carpetas de evidencias
- Revisión de evidencias individuales

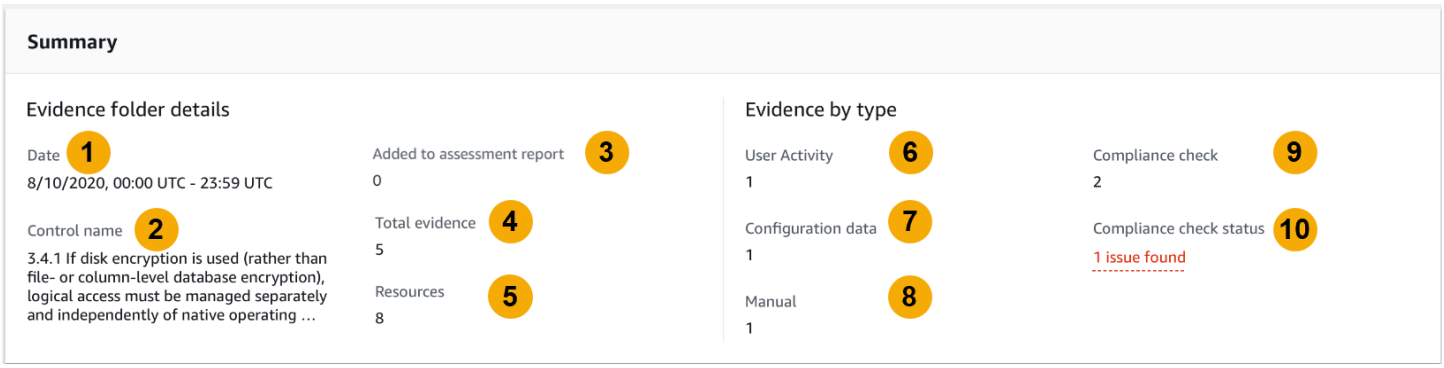
Revisión de las carpetas de evidencias

Al abrir una carpeta de evidencias verá una página de resumen de la misma que contiene dos secciones: un resumen y una tabla de evidencias. Veamos el contenido de cada una de las secciones.

- Resumen de la carpeta de evidencias
- Tabla de evidencias

Resumen de la carpeta de evidencias

El apartado de resumen de la página proporciona una visión general esquemática de las evidencias que contiene la carpeta.



Contiene la información siguiente:

1. Fecha muestra la fecha y hora de creación de la carpeta de evidencias, tiempo universal coordinado (UTC).
2. Nombre del control, es decir la denominación que recibe el control asociado a la carpeta de evidencias.
3. Agregado al informe de evaluación representa el número de evidencias que se seleccionó manualmente para incluirlas en el informe de evaluación.
4. Total de evidencias, es decir el número de evidencias de la carpeta de evidencias.
5. Recursos: el número total de recursos AWS que se evaluaron al generar las evidencias de la carpeta.
6. Actividad del usuario indica cuántas evidencias se incluyen en dicha categoría. Esta evidencia se recopila de los registros de AWS CloudTrail.
7. Datos de configuración hace referencia al número de evidencias que se incluyen en dicha categoría. Esta información proviene de instantáneas de configuración de otros Servicios de AWS, como Amazon EC2, Amazon S3 o IAM.
8. Manual, para el número de evidencias que se incluyen en dicha categoría. Estas evidencias se cargan manualmente.
9. Comprobación de conformidad hace referencia al número de evidencias que se incluyen en dicha categoría. Estas evidencias se recopilan de AWS Config o AWS Security Hub.
10. Estado de la comprobación de conformidad indica el número total de problemas que se denunciaron directamente desde AWS Security Hub, AWS Config, o de ambos.

> **Tip**
>
> Para más información sobre los distintos tipos de evidencias (actividad del usuario, datos de configuración, comprobación de conformidad y manual), consulte Evidencias.

Tabla de evidencias

La tabla de evidencias enumera las evidencias individuales que se encuentran en la carpeta de evidencias.

Contiene la información siguiente:

1. Hora especifica cuándo se recopiló la evidencia y, a su vez, sirve como nombre de esta. Se representa en formato de tiempo universal coordinado (UTC). Al elegir una hora de la columna, se abrirá una página de detalles de las evidencias. En las secciones siguientes se describe la información que encontrará en dicha página.
2. Evidencias por tipo indica la categoría de las evidencias.
   - Las evidencias de comprobación de conformidad se recopilan de AWS Config o AWS Security Hub.
   - Las evidencias de la actividad del usuario se recopilan de los registros de AWS CloudTrail.
   - Las evidencias de los datos de configuración se recopilan a partir de instantáneas de otros servicios, como Amazon EC2, Amazon S3 o IAM.
   - Las evidencias manuales son aquellas que se cargan manualmente.
3. Comprobación de conformidad: el estado de la evaluación de la evidencia o evidencias incluidas en dicha categoría.
   - En el caso de las evidencias recopiladas de AWS Security Hub, se informa de los resultados de aprobado o no aprobado directamente desde AWS Security Hub.
   - En el caso de las evidencias recopiladas de AWS Config, se informa de los resultados de conforme o no conforme directamente desde AWS Config.
   - Puede aparecer la opción No aplicable. Esto indica que, o bien no tiene AWS Security Hub o AWS Config habilitadas, o bien las evidencias provienen de un tipo de origen de datos diferente.
4. Origen de datos, es decir el origen de datos desde el cual se recopila las evidencias.
5. Nombre del evento, es decir el nombre del evento o eventos que se incluye en las evidencias.
6. Recursos incluidos hace referencia a cuántos recursos se han evaluado generar las evidencias.

7. Selección del informe de evaluación indica si la evidencia se seleccionó manualmente para incluirla en el informe de evaluación.
   - Para incluir evidencias, selecciónelas y elija Agregar al informe de evaluación.
   - Para excluirlas, seleccione la evidencia o evidencias y elija Eliminar del informe de evaluación.

Para cargar evidencias manuales en la carpeta de evidencias, elija Cargar evidencias manuales, introduzca su URI de S3 y, a continuación, elija Cargar. Para más información, consulte Agregar evidencias manuales en AWS Audit Manager.

Para ver los detalles de cualquier evidencia, elija su nombre siguiendo el un hipervínculo de la columna Hora. Se abrirá una página de detalles de la evidencia, que se describe en la sección siguiente.

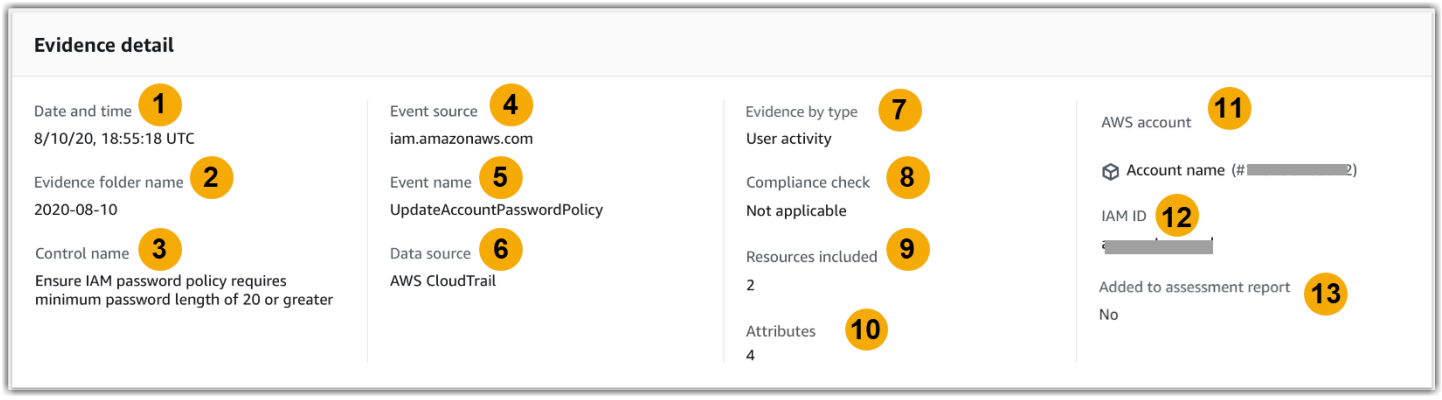
Revisión de evidencias individuales

Al abrir una evidencia individual verá una página de detalles de la evidencia que contiene tres secciones: los detalles de la evidencia, la tabla de atributos y la tabla de recursos incluidos. Veamos el contenido de cada una de las secciones.

- Detalle de las evidencias
- Atributos
- Recursos incluidos

Detalle de las evidencias

El apartado de detalles de las evidencias de esta página resume las evidencias.



Contiene la información siguiente:

1. Fecha y hora: especifica cuándo se recopiló la evidencia, representadas en tiempo universal coordinado (UTC).
2. Nombre de la carpeta de evidencias, es decir la denominación de la carpeta que contiene la evidencia o evidencias.
3. Nombre del control: el nombre del control asociado a la evidencia o evidencias.
4. Origen del evento: el nombre del recurso que creó el evento de la evidencia o evidencias.
5. Nombre del evento: el nombre del evento de la evidencia o evidencias.
6. Origen de datos: el origen de datos desde el cual se recopiló la evidencia.
7. Evidencia por tipo: el tipo de cada evidencia.
   - Las evidencias de comprobación de conformidad se recopilan de AWS Config o AWS Security Hub.
   - Las evidencias de la actividad del usuario se recopilan de los registros de AWS CloudTrail.
   - Las evidencias de los datos de configuración se recopilan a partir de instantáneas de otros Servicios de AWS, como Amazon EC2, Amazon S3 o IAM.
   - Las evidencias manuales son aquellas que se cargan manualmente.
8. Comprobación de conformidad: el estado de la evaluación de la evidencia o evidencias incluidas en dicha categoría.
   - En el caso de las evidencias recopiladas de AWS Security Hub, se informa de los resultados de aprobado o no aprobado directamente desde AWS Security Hub.
   - En el caso de las evidencias recopiladas de AWS Config, se informa de los resultados de conforme o no conforme directamente desde AWS Config.
   - Puede aparecer la opción No aplicable. Esto indica que, o bien no tiene AWS Security Hub o AWS Config habilitadas, o bien las evidencias provienen de un tipo de origen de datos diferente.
9. Recursos incluidos indica el número de recursos evaluados para generar la evidencia o evidencias.
10. Atributos muestra el total de atributos que utiliza el evento en la evidencia o evidencias.
11. Cuenta de AWS es la Cuenta de AWS de donde se recopiló la evidencia.
12. ID de IAM es el usuario o rol correspondiente, en caso aplicable.
13. Agregado al informe de evaluación: indica si ha optado por incluir las evidencias en el informe de evaluación.

Atributos

La tabla de atributos muestra los nombres y valores que utiliza el evento en la evidencia. Contiene la información siguiente:

- Nombre del atributo es el requisito de la evidencia, como allowUsersToChangePassword.
- Valor hace referencia al valor del atributo; por ejemplo verdadero o falso.

Recursos incluidos

La tabla de recursos incluidos muestra la lista de recursos evaluados para generar la evidencia o evidencias. Contiene uno o varios de los campos siguientes:

- ARN, el nombre de recurso de Amazon (ARN) del recurso o recursos. Es posible que el ARN no esté disponible para todos los tipos de evidencia.
- Valor, el valor de dicho recurso, en caso aplicable.
- JSON muestra el enlace para ver el archivo JSON del recurso o recursos.

Carga manual de evidencias en AWS Audit Manager

Audit Manager puede recopilar automáticamente evidencias para muchos controles. Sin embargo, para algunos de ellos deberá añadir sus propias evidencias manualmente.

Considere los siguientes ejemplos:

- Algunos controles se refieren al suministro de registros físicos (como firmas) o a eventos que no se generan en la nube (como observaciones y entrevistas). En estos casos, puede cargar manualmente los archivos como evidencia. Por ejemplo, si un control requiere información sobre la estructura corporativa, puede subir una copia del organigrama de su empresa como evidencia manual.
- Algunos controles representan preguntas de evaluación del riesgo de los proveedores. Las preguntas de evaluación de riesgos pueden requerir documentación como prueba (por ejemplo un organigrama) o quizá solo tenga que introducir una respuesta de texto simple, como una lista de puestos de trabajo. En este último caso, puede responder a la pregunta y guardar su respuesta como evidencia manual.

También puede utilizar la característica de carga manual para gestionar las evidencias de varios entornos. Si su empresa utiliza un modelo de nube híbrida o multinube, puede cargar evidencias desde su entorno local, desde entornos alojados en la nube o sus aplicaciones de SaaS. Esto le permite organizar sus evidencias independientemente de su procedencia, almacenándolas dentro de la estructura de una evaluación de Audit Manager, en la que cada prueba se asignará a un control específico.

Para más información sobre los distintos tipos de evidencia en Audit Manager, consulte Evidencias en el apartado de conceptos y terminología de esta guía.

Cómo añadir evidencias manuales

Aplique cualquiera de los métodos que se detallan a continuación para agregar sus propias evidencias manuales a los controles de evaluación.

Tenga en cuenta lo siguiente:

- Solo puede utilizar un método a la vez para agregar evidencias manuales.
- El tamaño máximo admitido para un único archivo de evidencia manual es de 100 MB.
- Los Formatos de archivo compatibles con las evidencias manuales se enumeran en esta misma página a continuación.
- Cada cuenta de Cuenta de AWS solo puede cargar manualmente hasta 100 archivos de pruebas a un control cada día. Si supera este límite diario no podrá realizar ninguna carga manual adicional en ese control. Si necesita cargar una gran cantidad de evidencias manuales en un solo control, hágalo en lotes durante varios días.
- Cuando un control está inactivo, no es posible añadir evidencias manuales a ese control. Para ello, primero debe cambiar el estado del control al estado de en revisión o revisado. Para obtener más información, consulte Actualización del estado de control.

Importar un archivo desde Amazon S3

Siga estos pasos para importar evidencias manuales desde un bucket de S3.

AWS console

Pasos para importar archivos de S3 (consola)

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.

2. En el panel de navegación izquierdo, elija Evaluaciones y, a continuación, el nombre de la evaluación que desee abrir.
3. Seleccione la pestaña Controles, desplácese hacia abajo hasta llegar a Conjuntos de controles y, a continuación, elija el nombre de un control para abrirlo.
4. En la pestaña Carpetas de evidencias, elija Añadir evidencia manual y, a continuación, Importar archivo de S3.
   - También puede seleccionar un nombre de carpeta de evidencias desde la pestaña Carpetas de evidencias para revisar el resumen de las mismas y, a continuación, elegir Añadir evidencia manual e Importar archivo de S3.
5. En la página siguiente, ingrese el URI de S3 de la evidencia. Para encontrar el URI de S3, vaya al objeto en la consola de Amazon S3 y elija Copiar URI de S3.
6. Seleccione Cargar.

AWS CLI

Después, reemplace el *texto del marcador de posición* por su información según corresponda.

Pasos para importar un archivo de S3 (CLI)

1. Ejecute el comando `list-assessments` para ver una lista de sus evaluaciones.

```
aws auditmanager list-assessments
```

   En la respuesta, busque la evaluación de la que desee cargar la evidencia o evidencias y anote sus identificadores.
2. Ejecute el comando `get-assessment` y especifique el ID de evaluación del primer paso.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

   En la respuesta, busque el conjunto de controles y el control en el que desee cargar las evidencias y anote sus identificadores.
3. Use el comando `batch-import-evidence-to-assessment-control` con estos parámetros:

- `--assessment-id`: utilice el ID de evaluación del primer paso.
- `--control-set-id`: utilice el ID del conjunto de controles del segundo paso.
- `--control-id`: utilice el ID de control del segundo paso.
- `--manual-evidence`: utilice `s3ResourcePath` como tipo de evidencia manual y especifique el URI de S3 de la evidencia. Para encontrar el URI de S3, vaya al objeto en la consola de Amazon S3 y elija Copiar URI de S3.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence s3ResourcePath=s3://
example-bucket/example-file.extension
```

Audit Manager API

Pasos para importar un archivo desde S3 (API)

1. Llame a la operación `ListAssessments` para ver una lista de sus evaluaciones. En la respuesta, busque la evaluación de la que desee cargar la evidencia o evidencias y anote sus identificadores.
2. Llame a la operación `GetAssessment` y especifique el ID de evaluación del primer paso. En la respuesta, busque el conjunto de controles y el control en el que desee cargar las evidencias y anote sus identificadores.
3. Realice una llamada a la operación `BatchImportEvidenceToAssessmentControl` con los parámetros siguientes:
   - `assessmentId`: utilice el ID de evaluación del primer paso.
   - `controlSetId`: utilice el ID del conjunto de controles del segundo paso.
   - `controlId`: utilice el ID de control del segundo paso.
   - `manualEvidence`: utilice `s3ResourcePath` como tipo de evidencia manual y especifique el URI de S3 de la evidencia. Para encontrar el URI de S3, vaya al objeto en la consola de Amazon S3 y elija Copiar URI de S3.

Consulte cualquiera de los enlaces anteriores para obtener más información en la referencia de la API de AWS Audit Manager. Esto incluye información sobre el uso de estas operaciones y parámetros en un lenguaje específico de los SDK de AWS.

Cargar un archivo desde el navegador

Siga estos pasos para cargar evidencias manualmente desde su navegador.

AWS console

Pasos para cargar archivos desde el navegador (consola)

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija Evaluaciones y, a continuación, el nombre de la evaluación que desee abrir.
3. En la pestaña Controles, desplácese hacia abajo hasta llegar a Conjuntos de controles y, a continuación, elija el nombre del control que desee abrir.

   A partir de este punto, hay tres formas de cargar un archivo:

   - (Opción 1) En el banner de notificación azul, seleccione Cargar evidencias manuales.
   - (Opción 2) En la pestaña Carpetas de evidencias, seleccione Agregar evidencias manuales y, a continuación, Cargar archivos desde el navegador.
   - (Opción 3) Elija el nombre de una carpeta de evidencias para revisar un resumen del contenido de la carpeta. A continuación elija Agregar evidencias manuales y Cargar archivos desde el navegador.
4. Seleccione el archivo en el cual desee cargar los archivos.
5. Seleccione Cargar.

AWS CLI

Después, reemplace el *`texto del marcador de posición`* por su información según corresponda.

Pasos para cargar archivos desde su navegador (CLI)

1. Ejecute el comando `list-assessments` para ver una lista de sus evaluaciones.

```
aws auditmanager list-assessments
```

En la respuesta, busque la evaluación de la que desee cargar la evidencia o evidencias y anote sus identificadores.

2. Ejecute el comando `get-assessment` y especifique el ID de evaluación del primer paso.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

En la respuesta, busque el conjunto de controles y el control en el que desee cargar las evidencias y anote sus identificadores.

3. Ejecute el comando `get-evidence-file-upload-url` y especifique el archivo o archivos que desea cargar.

```
aws auditmanager get-evidence-file-upload-url --file-name fileName.extension
```

En la respuesta, busque y anote la URL prefirmada y `evidenceFileName`.

4. Use la URL prefirmada del tercer paso para cargar el archivo o archivos desde su navegador. Esta acción carga los archivos en Amazon S3, donde se guardan como un objeto que se puede agregar a los controles de evaluación. En el siguiente paso haga referencia al objeto recién creado mediante el parámetro `evidenceFileName`.

> **Note**
>
> Cuando carga un archivo mediante una URL prefirmada, Audit Manager protege y almacena sus datos mediante el cifrado del servidor con AWS Key Management Service. Para ello, debe utilizar el encabezado `x-amz-server-side-encryption` en su solicitud cuando utilice la URL prefirmada para cargar el archivo.
> Si utiliza un cliente gestionado AWS KMS key en la configuración de Cifrado de datos de Audit Manager, asegúrese de incluir también el encabezado `x-amz-server-side-encryption-aws-kms-key-id` en su solicitud. Si el encabezado `x-amz-server-side-encryption-aws-kms-key-id` no figura en la solicitud, Amazon S3 asumirá que se quiere utilizar la Clave administrada de AWS.

Para más información, consulte Protección de los datos con el cifrado del servidor con claves AWS Key Management Service de KMS (SSE-KMS) en la guía del usuario de Amazon Simple Storage Service.

5. Use el comando `batch-import-evidence-to-assessment-control` con estos parámetros:

   - `--assessment-id`: utilice el ID de evaluación del primer paso.
   - `--control-set-id`: utilice el ID del conjunto de controles del segundo paso.
   - `--control-id`: utilice el ID de control del segundo paso.
   - `--manual-evidence`: utilice `evidenceFileName` como tipo de evidencia manual y especifique el nombre del archivo de la evidencia o evidencias a partir del tercer paso.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet
 --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence
 evidenceFileName=fileName.extension
```

Audit Manager API

Pasos para cargar archivos desde su navegador (API)

1. Llame a la operación `ListAssessments`. En la respuesta, busque la evaluación de la que desee cargar la evidencia o evidencias y anote sus identificadores.
2. Llame a la `GetAssessment` operación y especifique el `assessmentId` del primer paso. En la respuesta, busque el conjunto de controles y el control en el que desee cargar las evidencias y anote sus identificadores.
3. Llame a la operación `GetEvidenceFileUploadUrl` y especifique el `fileName` que desea cargar. En la respuesta, busque y anote la URL prefirmada y `evidenceFileName`.
4. Use la URL prefirmada del tercer paso para cargar el archivo o archivos desde su navegador. Esta acción carga los archivos en Amazon S3, donde se guardan como un objeto que se puede agregar a los controles de evaluación. En el siguiente paso haga referencia al objeto recién creado mediante el parámetro `evidenceFileName`.

> **Note**
>
> Cuando carga un archivo mediante una URL prefirmada, Audit Manager protege y almacena sus datos mediante el cifrado del servidor con AWS Key Management Service. Para ello, debe utilizar el encabezado `x-amz-server-side-encryption` en su solicitud cuando utilice la URL prefirmada para cargar el archivo.
> Si utiliza un cliente gestionado AWS KMS key en la configuración de Cifrado de datos de Audit Manager, asegúrese de incluir también el encabezado `x-amz-server-side-encryption-aws-kms-key-id` en su solicitud. Si el encabezado `x-amz-server-side-encryption-aws-kms-key-id` no figura en la solicitud, Amazon S3 asumirá que se quiere utilizar la Clave administrada de AWS.
> Para más información, consulte Protección de los datos con el cifrado del servidor con claves AWS Key Management Service de KMS (SSE-KMS) en la guía del usuario de Amazon Simple Storage Service.

5. Realice una llamada a la operación `BatchImportEvidenceToAssessmentControl` con los parámetros siguientes:

   - `assessmentId`: utilice el ID de evaluación del primer paso.
   - `controlSetId`: utilice el ID del conjunto de controles del segundo paso.
   - `controlId`: utilice el ID de control del segundo paso.
   - `manualEvidence`: utilice `evidenceFileName` como tipo de evidencia manual y especifique el nombre del archivo de la evidencia o evidencias a partir del tercer paso.

Consulte cualquiera de los enlaces anteriores para obtener más información en la referencia de la API de AWS Audit Manager. Esto incluye información sobre el uso de estas operaciones y parámetros en un lenguaje específico de los SDK de AWS.

Introducción de una respuesta de texto

Siga estos pasos para introducir una respuesta a una pregunta de evaluación de riesgos y guarde su respuesta como prueba manual.

AWS console

Pasos para introducir una respuesta de texto (consola)

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija Evaluaciones y, a continuación, el nombre de la evaluación que desee abrir.
3. Seleccione la pestaña Controles, desplácese hacia abajo hasta llegar a Conjuntos de controles y, a continuación, elija el nombre de un control para abrirlo.

   A partir de este punto, hay tres formas de introducir una respuesta de texto:

   - (Opción 1) En el banner de notificación azul, seleccione Agregar respuesta.
   - (Opción 2) En la pestaña Carpetas de evidencias, elija Agregar evidencias manuales y, a continuación, Introducir respuesta de texto.
   - (Opción 3) Elija una carpeta de evidencias para revisar un resumen de su contenido, elija Agregar evidencia manual y, a continuación, Agregar respuesta de texto.
4. Aparecerá una ventana emergente que aparece: introduzca su respuesta en formato de texto plano.
5. Seleccione Confirmar.

AWS CLI

Después, reemplace el *texto del marcador de posición* por su información según corresponda.

Pasos para introducir una respuesta de texto (CLI)

1. Ejecute el comando `list-assessments`.

   ```
   aws auditmanager list-assessments
   ```

   En la respuesta, busque la evaluación de la que desee cargar la evidencia o evidencias y anote sus identificadores.
2. Ejecute el comando `get-assessment` y especifique el ID de evaluación del primer paso.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

En la respuesta, busque el conjunto de controles y el control en los que desee cargar las evidencias y anote sus identificadores.

3. Use el comando batch-import-evidence-to-assessment-control con estos parámetros:

   - `--assessment-id`: utilice el ID de evaluación del primer paso.
   - `--control-set-id`: utilice el ID del conjunto de controles del segundo paso.
   - `--control-id`: utilice el ID de control del segundo paso.
   - `--manual-evidence`: utilice `textResponse` como evidencia manual e introduzca el texto que desee guardar como evidencia manual.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence textResponse="enter
 text here"
```

Audit Manager API

Pasos para introducir una respuesta de texto (API)

1. Llame a la operación ListAssessments. En la respuesta, busque la evaluación de la que desee cargar la evidencia o evidencias y anote sus identificadores.
2. Llame a la GetAssessment operación y especifique el `assessmentId` del primer paso. En la respuesta, busque el conjunto de controles y el control en los que desee cargar las evidencias y anote sus identificadores.
3. Realice una llamada a la operación BatchImportEvidenceToAssessmentControl con los parámetros siguientes:

   - assessmentId: utilice el ID de evaluación del primer paso.
   - controlSetId: utilice el ID del conjunto de controles del segundo paso.
   - controlId: utilice el ID de control del segundo paso.

- `manualEvidence`: utilice `textResponse` como evidencia manual e introduzca el texto que desee guardar como evidencia manual.

Consulte cualquiera de los enlaces anteriores para obtener más información en la referencia de la API de AWS Audit Manager. Esto incluye información sobre el uso de estas operaciones y parámetros en un lenguaje específico de los SDK de AWS.

Formatos de archivo compatibles con las evidencias manuales

En la siguiente tabla se enumeran y describen los tipos de archivos que puede cargar como evidencia manual. Para cada tipo de archivo, se incluyen también las extensiones de los archivos compatibles.

Tipo de archivo	Descripción	Extensiones de archivos compatibles
Compresión o archivos	Archivos comprimidos GNU Zip y archivos comprimidos ZIP	`.gz`, `.zip`
Documento	Archivos de documentos comunes, como archivos PDF y Microsoft Office	`.doc`, `.docx`, `.pdf`, `.ppt`, `.pptx`, `.xls`, `.xlsx`
Imagen	Archivos de imágenes y gráficos	`.jpeg`, `.jpg`, `.png`, `.svg`
Texto	Otros archivos de texto no binarios, como documentos de texto sin formato y archivos de lenguaje de marcado	`.cer`, `.csv`, `.html`, `.jmx`, `.json`, `.md`, `.out`, `.rtf`, `.txt`, `.xml`, `.yaml`, `.yml`

Generación de informes de evaluación

Los informes de evaluación resumen su evaluación e incluyen enlaces a un conjunto organizado de carpetas que contienen evidencias relacionadas. Para obtener más información, consulte Informes de evaluación.

Puede elegir qué evidencias desea incluir en los informes de evaluación antes de generarlos. Las evidencias recién recopiladas no se incluyen automáticamente en los informes de evaluación.

Tareas

- Añadir evidencias a los informes de evaluación
- Eliminación de evidencias de un informe de evaluación
- Generación de informes de evaluación
- ¿Cuál es el siguiente paso?

Añadir evidencias a los informes de evaluación

Para poder generar un informe de evaluación, debe agregar al menos un elemento de evidencia a dicho informe. Puede añadir una carpeta de evidencias completa o elementos de evidencia individuales desde una carpeta.

Pasos para añadir evidencias a un informe de evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Evaluaciones y, a continuación, el nombre de la evaluación o evaluaciones que desee abrir.
3. En la pestaña Controles, desplácese hacia abajo hasta llegar a la tabla Conjuntos de controles y elija el nombre del control o controles que desee abrir.
4. Elija cómo quiere añadir las evidencias a su informe de evaluación.

    a. Para añadir carpetas de evidencias completas, desplácese hacia abajo hasta llegar a Carpetas de evidencias, seleccione la que desee añadir y, a continuación, elija Añadir al informe de evaluación.

        - Si no ve la carpeta que busca, cambie el filtro desplegable a Siempre. Tenga en cuenta que por defecto se muestran las carpetas de los últimos siete días.

- Si la opción Añadir al informe de evaluación aparece atenuada, significa que la carpeta de evidencias ya se ha añadido a dicho informe.

b. Para añadir evidencias específicas, elija una carpeta de evidencias y ábrala. Seleccione uno o más elementos de la lista y, a continuación, elija Añadir al informe de evaluación.

- Si la opción Añadir al informe de evaluación aparece atenuada, asegúrese de haber seleccionado la casilla de verificación situada junto a las evidencias e inténtelo de nuevo.

5. Una vez añadidas las evidencias al informe de evaluación, aparecerá un aviso de confirmación en verde. Seleccione Ver evidencias en el informe de evaluación para ver las evidencias que se incluirán en su informe de evaluación.

- También puede consultarlas desde la pestaña de selección del informe de evaluación si vuelve a la evaluación.

Eliminación de evidencias de un informe de evaluación

Siga los pasos que se detallan a continuación para eliminar evidencias de un informe de evaluación. Puede eliminar carpetas de evidencias completas o elementos de evidencia específicos de una carpeta.

Pasos para eliminar evidencias de un informe de evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Evaluaciones y, a continuación, el nombre de la evaluación o evaluaciones que desee abrir.
3. En la pestaña Controles, desplácese hacia abajo hasta llegar a la tabla Conjuntos de controles y elija el nombre del control o controles que desee abrir.
4. Elija cómo desea eliminar las evidencias del informe de evaluación.

a. Para eliminar una carpeta de evidencias completa, desplácese hacia abajo hasta llegar a Carpetas de evidencias. A continuación, seleccione la carpeta que desee eliminar y elija Eliminar del informe de evaluación.

- Si no ve la carpeta que busca, cambie el filtro desplegable a Siempre. Tenga en cuenta que por defecto se muestran las carpetas de los últimos siete días.

- Si Eliminar del informe de evaluación aparece atenuada, significa que la carpeta de evidencias ya se ha eliminado del informe de evaluación.

b. Para eliminar evidencias específicas, elija una carpeta de evidencias y ábrala. Seleccione uno o más elementos de la lista y, a continuación, elija Eliminar del informe de evaluación.

- Si la opción Eliminar del informe de evaluación aparece atenuada, asegúrese de haber seleccionado la casilla de verificación situada junto a las evidencias e inténtelo de nuevo.

5. Una vez añadidas las evidencias al informe de evaluación, aparecerá un aviso de confirmación en verde. Seleccione Ver evidencias en el informe de evaluación para ver las evidencias que se incluirán en su informe de evaluación.
   - También puede consultarlas desde la pestaña de selección del informe de evaluación si vuelve a la evaluación.

Generación de informes de evaluación

Puede generar el informe de evaluación final para compartirlo con los auditores después de añadir las evidencias que corresponda. Cuando genera un informe de evaluación, se coloca en el bucket de S3 que haya elegido como destino del informe de evaluación.

> **Tip**
>
> Para asegurarse de que su informe de evaluación se haya generado correctamente, consulte nuestro Consejos de configuración para el destino de su informe de evaluación.

Para generar un informe de evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación de la izquierda, elija Evaluaciones.
3. Elija el nombre de la evaluación para la que desea generar un informe de evaluación.
4. Vaya a la pestaña de selección del informe de evaluación y, a continuación, Generar informe de evaluación.
   - Si la opción Generar informe de evaluación aparece atenuada, significa que aún no se ha añadido ninguna prueba a dicho informe.

5. En la ventana emergente, agregue un nombre y una descripción para el informe de evaluación y revise los detalles del mismo.
6. Elija Generar informe de evaluación y espere unos minutos mientras se genera.
7. Busque y descargue su informe de evaluación desde el centro de descargas de la consola Audit Manager.
    - También puede ir al bucket de S3 de destino del informe de evaluación y descargar el informe de evaluación desde allí.

El informe de evaluación incluye una suma de comprobación de archivos para garantizar la integridad del informe de evaluación. Puede validarlo con la operación de la API de Audit Manager ValidateAssementReportIntegrity.

¿Cuál es el siguiente paso?

Después de generar el informe de evaluación, puede seguir con otros pasos. Descúbralos a continuación:

- Busque y descargue su informe de evaluación: aprenda cómo descargar su informe de evaluación desde el centro de descargas o desde Amazon S3.
- Explore su informe de evaluación: aprenda cómo navegar por un informe de evaluación y conozca su contenido.
- Valide su informe de evaluación: aprenda cómo utilizar la operación de la API ValidateAssessmentReportIntegrity para validar sus informes.
- Eliminar un informe de evaluación no deseado: aprenda cómo eliminar informes que no necesite del centro de descargas o de Amazon S3.

Cambio del estado de las evaluaciones a inactivas

Si ya no necesita recopilar pruebas para una evaluación, puede cambiar el estado de la evaluación a Inactiva. Cuando el estado de una evaluación cambia a inactiva, la evaluación deja de recopilar pruebas. Como resultado, ya no se le cobrará nada por esa evaluación.

Además de detener la recopilación de evidencias, Audit Manager realiza los siguientes cambios en los controles de las evaluaciones inactivas:

- Todos los conjuntos de controles cambian al estado revisado.

- Todos los controles que están en revisión cambian al estado revisado.
- Los delegados de la evaluación inactiva ya no pueden ver ni editar sus controles ni conjuntos de controles.

> **Warning**
>
> Esta acción es irreversible. Le recomendamos que proceda con cautela y se asegure de marcar estas evaluaciones como inactivas. Cuando una evaluación está inactiva, tiene acceso de solo lectura a su contenido. Esto significa que aún puede ver las pruebas recopiladas anteriormente y generar informes de evaluación. Sin embargo, no puede editar la evaluación inactiva, agregar comentarios ni cargar ninguna prueba manual.

Audit Manager console

Pasos para cambiar el estado de las evaluaciones a inactiva (consola)

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Evaluaciones.
3. Seleccione el nombre de la evaluación que desee consultar y ábrala.
4. En la esquina superior derecha de la página, elija Actualizar estado de la evaluación y, luego, Inactivo.
5. Seleccione Actualizar estado en la ventana emergente para confirmar que desea cambiar el estado a inactivo.

Los cambios en las evaluaciones y sus controles surten efecto después de un minuto aproximadamente.

AWS CLI

Pasos para cambiar el estado de las evaluaciones a inactiva (AWS CLI)

1. En primer lugar, identifique la evaluación o evaluaciones que desea actualizar. Para ello, ejecute el comando list-assessments.

```
aws auditmanager list-assessments
```

Obtendrá una lista de evaluaciones. Busque la evaluación o evaluaciones que desee desactivar y tome nota de su identificador.

2. Ahora ejecute el comando update-assessment-status y especifique los siguientes parámetros:

   - `--assessment-id`, para determinar qué evaluación o evaluaciones desea desactivar.
   - `--status`: establezca este valor en `INACTIVE`.

   En el siguiente ejemplo, reemplace el *`texto de marcador`* con su información, según corresponda.

   ```
   aws auditmanager update-assessment-status --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --status INACTIVE
   ```

Los cambios en las evaluaciones y sus controles surten efecto después de un minuto aproximadamente.

Audit Manager API

Pasos para cambiar el estado de las evaluaciones a inactivas (API)

1. Utilice la operación ListAssessments para buscar la evaluación o evaluaciones que desea desactivar y anote su identificador.
2. Utilice la operación UpdateAssessmentStatus y especifique los siguientes parámetros:

   - ID de evaluación, para determinar qué evaluación o evaluaciones desea desactivar.
   - estatus: defina este valor como `INACTIVE`.

Los cambios en las evaluaciones y sus controles surten efecto después de un minuto aproximadamente.

Para más información sobre estas operaciones de la API, consulte cualquiera de los enlaces anteriores en la referencia de la API de AWS Audit Manager. Esto incluye información sobre el uso de estas operaciones y parámetros en un lenguaje específico de los SDK de AWS.

Eliminación de las evaluaciones

Puede eliminar las evaluaciones de Audit Manager que ya no necesite. Puede eliminar evaluaciones utilizando la consola de Audit Manager, la API de Audit Manager o la AWS Command Line Interface (AWS CLI).

> **Warning**
>
> Esta acción elimina de manera permanente la evaluación y todas las pruebas recopiladas en ella. No puede recuperar estos datos. Por ello, le recomendamos que proceda con cuidado y que esté seguro de que desea eliminar la evaluación.

Audit Manager console

Pasos para eliminar evaluaciones (consola)

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Evaluaciones.
3. Seleccione las evaluaciones que desee eliminar y elija Eliminar.
   - También puede abrirlas y elegir Eliminar en la parte superior derecha de la página.

AWS CLI

Pasos para eliminar evaluaciones (AWS CLI)

1. Primero identifique las evaluaciones que desee eliminar. Para ello, ejecute el comando list-assessments.

   ```
   aws auditmanager list-assessments
   ```

   Obtendrá una lista de evaluaciones. Busque la evaluación o evaluaciones que desee eliminar y tome nota de su identificador.
2. A continuación, ejecute el comando delete-assessment y especifique el `--assessment-id` de la evaluación o evaluaciones que desea eliminar.

En el siguiente ejemplo, reemplace el *texto de marcador* con su información, según corresponda.

```
aws auditmanager delete-assessment --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Pasos para eliminar evaluaciones (API)

1. Utilice la operación ListAssessments para buscar la evaluación o evaluaciones que desea eliminar.

   En la respuesta, busque y anote el ID de evaluación.
2. Utilice la operación DeleteAssessment y especifique el ID de evaluación de la evaluación o evaluaciones que desee eliminar.

Para más información sobre estas operaciones de la API, consulte cualquiera de los enlaces anteriores en la referencia de la API de AWS Audit Manager. Esto incluye información sobre el uso de estas operaciones y parámetros en un lenguaje específico de los SDK de AWS.

> **Tip**
>
> Si su objetivo es reducir los costos, considere la posibilidad de cambiar el estado de la evaluación a inactiva en lugar de eliminarla. Esta acción detiene la recopilación de pruebas y establece que la evaluación esté en un estado de solo lectura en el que puede revisar las pruebas recopiladas anteriormente. Las evaluaciones inactivas no generan ningún cargo.

Delegación en AWS Audit Manager

Los propietarios de la auditoría utilizan AWS Audit Manager para crear evaluaciones y recopilar evidencias para los controles que figuran en esa evaluación. A veces, los propietarios de las auditorías pueden tener dudas o necesitar ayuda a la hora de validar la prueba de un conjunto de controles. En esta situación, el propietario de una auditoría puede delegar un conjunto de controles en un experto en la materia para su revisión.

En líneas generales, el proceso de delegación es el siguiente:

1. El propietario de la auditoría elige un conjunto de controles en su evaluación y lo delega para su revisión.
2. El delegado revisa esos controles y sus evidencias, y devuelve el conjunto de controles al propietario de la auditoría una vez finalizado.
3. Se notifica al propietario de la auditoría que la revisión ha finalizado y comprueba los controles revisados para comprobar si hay comentarios del delegado.

Utilice las siguientes secciones de esta guía para obtener más información sobre cómo gestionar las tareas de delegación en AWS Audit Manager.

Temas

> **Note**
>
> Una cuenta puede ser el propietario de una auditoría o un delegado en distintas regiones AWS.

Delegación de tareas para los propietarios de auditorías

Como propietario de una auditoría en AWS Audit Manager, es posible que necesite la ayuda de un experto en la materia que le ayude a revisar los controles y las evidencias. En esta situación, puede delegar la revisión de un conjunto de controles.

En los temas siguientes, se describe cómo se pueden gestionar las delegaciones en AWS Audit Manager.

Tareas de delegación

- Delegación de conjuntos de controles para su revisión
- Acceder a sus delegaciones activas y finalizadas
- Borrar las delegaciones activas y finalizadas

Delegación de conjuntos de controles para su revisión

Cuando necesite la ayuda de un experto en la materia, puede elegir la cuenta AWS en la cuenta que desea que le ayude y delegarle un conjunto de controles para que los revise.

Puede utilizar uno de los procedimientos siguientes para delegar un conjunto de controles.

Delegación de un conjunto de controles desde una página de evaluación

Para delegar un conjunto de controles de la página de evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Evaluaciones.
3. Seleccione el nombre de la evaluación que contiene el conjunto de controles que desea delegar.
4. En la página de evaluación, seleccione la pestaña Controles. Aquí se muestra el resumen del estado del control y la lista de controles de la evaluación.
5. Seleccione un conjunto de controles y elija Delegar el conjunto de controles.
6. En Selección de delegados, se muestra una lista de usuarios y roles. Elija un usuario o un rol, o utilice la barra de búsqueda para buscar uno.
7. En Detalles de la delegación, revise el nombre del conjunto de controles y el nombre de la evaluación.
8. (Opcional) En Comentarios, agregue un comentario con instrucciones para ayudar al delegado a realizar su tarea de revisión. No incluya información confidencial en su comentario.
9. Elija el conjunto de controles delegados.
10. Un cartel verde confirma que el conjunto de controles se ha delegado correctamente. Seleccione Ver delegación para ver la solicitud de delegación. También puede ver sus delegaciones en

cualquier momento al elegir Delegaciones del panel de navegación izquierdo de la consola AWS Audit Manager.

Delegar un conjunto de controles desde la página de delegaciones

Para delegar un conjunto de controles desde la página de delegaciones

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Delegación.
3. En la página de delegaciones, elija Crear delegación.
4. En Elegir el conjunto de evaluación y control, especifique la evaluación y el conjunto de controles que desea delegar.
5. En Selección de delegados, verá una lista de usuarios y funciones. Elija un usuario o un rol, o utilice la barra de búsqueda para buscar uno.
6. (Opcional) En Comentarios, agregue un comentario con instrucciones para ayudar al delegado a realizar su tarea de revisión. No incluya información confidencial en el alias de la cuenta.
7. Elija Crear delegación.
8. Un cartel verde confirma que el conjunto de controles se ha delegado correctamente. Seleccione Ver delegación para ver la solicitud de delegación. También puede ver sus delegaciones en cualquier momento al elegir Delegaciones del panel de navegación izquierdo de la consola AWS Audit Manager.

Al delegar la revisión de un conjunto de controles, el delegado recibe una notificación y, a continuación, puede empezar a revisar el conjunto de controles. Este proceso que siguen los delegados se describe en Tareas de delegación para los delegados.

> **Tip**
>
> Los delegados pueden suscribirse a un tema del SNS para recibir alertas por correo electrónico cuando se les delegue una tarea de revisión. Para obtener más información sobre cómo identificar y suscribirse al tema SNS asociado a AWS Audit Manager, consulte Notificaciones en AWS Audit Manager.

Acceder a sus delegaciones activas y finalizadas

Puede acceder a una lista de sus delegaciones en cualquier momento seleccionando Delegaciones en el panel de navegación izquierdo de AWS Audit Manager. La página de delegaciones contiene una lista de sus delegaciones activas y completas, con los siguientes detalles para cada delegación:

- Delegado a: la cuenta de AWS en la que ha delegado el conjunto de controles.
- Fecha: la fecha en la que delegó el conjunto de controles.
- Estado: el estado actual de la delegación.
- Evaluación: el nombre de la evaluación con un enlace a la página de detalles de la evaluación.
- Conjunto de controles: el nombre del conjunto de controles cuya revisión se delegó.

Cuando se complete una delegación, recibirá una notificación AWS Audit Manager. También puede recibir comentarios con comentarios del delegado. El siguiente procedimiento explica cómo comprobar las notificaciones en Audit Manager una vez finalizada la delegación y cómo ver los comentarios que el delegado haya dejado para usted.

Para ver una delegación completa y comprobar si hay comentarios

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Notificaciones. O elija Notificaciones en la barra flash azul de la parte superior de la pantalla para abrir la página de notificaciones.
3. Consulte la página de Notificaciones, que incluye una tabla con la siguiente información:
   - Fecha: fecha de la notificación.
   - Evaluación: el nombre de la evaluación asociada al conjunto de controles.
   - Conjunto de controles: el nombre del conjunto de controles.
   - Origen: el usuario o el rol del delegado que le devolvió el conjunto de controles completo.
   - Descripción: comentarios de alto nivel proporcionados por el delegado.
4. Busque el conjunto de evaluación y control que el delegado revisó y le envió y elija el nombre de la evaluación para abrirla.
5. En la pestaña Controles de la página de detalles de la evaluación, desplácese hacia abajo hasta la tabla de conjuntos de controles. En la columna Controles agrupados por conjunto, expanda el

nombre de un conjunto de controles para mostrar sus controles. A continuación, elija el nombre de un control para abrir la página de detalles del control.

6. Seleccione la pestaña Comentarios para ver los comentarios agregados por el delegado a ese control en particular.
7. Cuando esté seguro de que se ha completado la revisión de un conjunto de controles, seleccione el conjunto de controles y elija Completar la revisión del conjunto de controles.

> **Important**
>
> Audit Manager recopila evidencias de forma continua. Como resultado, es posible que se recopilen nuevas evidencias adicionales después de que el delegado complete la revisión de un control.
> Si solo desea utilizar las evidencias revisadas en sus informes de evaluación, puede consultar la marca temporal revisada por el control para determinar cuándo se revisó la evidencia. Esta marca de tiempo se encuentra en la pestaña Registro de cambios de la página de detalles del control. A continuación, puede utilizar esta marca de tiempo para identificar las evidencias que va a añadir a sus informes de evaluación.

Borrar las delegaciones activas y finalizadas

Puede haber circunstancias en las que cree una delegación, pero más adelante ya no necesite ayuda para revisar ese conjunto de controles. Cuando esto ocurra, puede eliminar una delegación activa en AWS Audit Manager. También puede eliminar las delegaciones completadas que ya no desee que aparezcan en la página de delegaciones.

Para eliminar una delegación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Delegaciones.
3. En la página Delegaciones, seleccione la delegación que desee cancelar y, a continuación, elija Eliminar delegación.
4. En la ventana emergente que aparece, elija Eliminar para confirmar su elección.

Tareas de delegación para los delegados

Los delegados suelen tener experiencia empresarial o técnica especializada en varias áreas diferentes. Estos incluyen políticas de retención de datos, planes de capacitación, infraestructura de red y administración de identidades. Pueden ayudar a los responsables de la auditoría a revisar las evidencias recopiladas para detectar los controles que entran en su área de especialización.

Como delegado, es posible que reciba solicitudes de los propietarios de la auditoría para revisar las evidencias asociadas a un conjunto de controles. Esta solicitud indica que el propietario de la auditoría necesita su ayuda para validar esta evidencia. Puede ayudar a los propietarios de la auditoría revisando los conjuntos de controles y sus evidencias relacionadas, añadiendo comentarios, cargando evidencias adicionales y actualizando el estado de cada control que revise.

En los temas siguientes, se describe cómo se pueden gestionar las delegaciones en AWS Audit Manager.

> **Note**
>
> Los propietarios de las auditorías delegan conjuntos de control específicos para su revisión, no para realizar evaluaciones completas. En consecuencia, los delegados tienen acceso limitado a las evaluaciones. Los delegados pueden revisar las evidencias, añadir comentarios, cargar evidencias manuales y actualizar el estado de control de cada uno de los controles del conjunto de controles. Para obtener más información acerca de los roles y sus permisos en Audit manager, consulte Políticas recomendadas para los usuarios de AWS Audit Manager.

Tareas de delegación

- Ver las notificaciones de las solicitudes de delegación entrantes
- Revisión del conjunto de control delegado y su evidencia relacionada
- Añadir un comentario a un control
- Marcar un control como revisado
- Volver a enviar el conjunto de controles revisado al propietario de la auditoría

Ver las notificaciones de las solicitudes de delegación entrantes

Cuando el propietario de una auditoría solicita su ayuda para revisar un conjunto de controles, usted recibe una notificación que le informa del conjunto de controles que le han delegado.

> **Tip**
>
> También puede suscribirse a un tema de SNS para recibir alertas por correo electrónico cuando se le delegue un conjunto de controles para su revisión. Para obtener más información, consulte Notificaciones de AWS Audit Manager.

Ver las notificaciones

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija Notificaciones. O bien, en la barra flash azul de la parte superior de la pantalla, elija Ver notificación para abrir la página de notificaciones.
3. En la página de Notificaciones, revise la lista de conjuntos de controles que se le han delegado para su revisión. La tabla incluye la siguiente información:
   - Fecha: la fecha en la que se delegó el conjunto de controles.
   - Evaluación: el nombre de la evaluación asociada al conjunto de controles.
   - Conjunto de controles: el nombre del conjunto de controles.
   - Origen: el usuario o rol que le delegó el conjunto de controles.
   - Descripción: instrucciones proporcionadas por el propietario de la auditoría.

Revisión del conjunto de control delegado y su evidencia relacionada

Puede ayudar a los propietarios de la auditoría revisando los conjuntos de controles que le han delegado. Puede examinar estos controles y la evidencia relacionada con ellos para determinar si es necesaria alguna acción adicional. Esta acción adicional podría incluir cargar manualmente evidencias adicionales para mostrar el cumplimiento o dejar un comentario en el que se detallen las medidas correctivas que ha seguido.

Para revisar un conjunto de controles

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Notificaciones. O bien, en la barra flash azul, selecciona Ver notificación para abrir la página de notificaciones.
3. En la página de Notificaciones, aparece una lista de los conjuntos de controles que se le han delegado. Identifique el conjunto de controles que desea revisar y elija el nombre de la evaluación relacionada para abrir la página de detalles de la evaluación.
4. En la pestaña Controles de la página de detalles de la evaluación, desplácese hacia abajo hasta la tabla de Conjuntos de controles.
5. En la columna Controles agrupados por conjunto de controles, expanda el nombre de un conjunto de controles para mostrar sus controles y elija el nombre de un control para abrir la página de detalles del control.
6. (Opcional) Seleccione Actualizar el estado del control para cambiar el estado del control. Mientras la revisión esté en curso, puede marcar el estado como En revisión.
7. Revise la información sobre el control en las pestañas de Carpetas de evidencias, Origen de datos, Comentarios y Registro de cambios. Para obtener información sobre cada una de estas pestañas y sobre cómo interpretarla, consulte Revisar los controles de una evaluación.

Para revisar la prueba de un control

1. En la página de detalles del control, seleccione la pestaña Carpetas de evidencias.
2. Navegue hasta la tabla de Carpetas de evidencias, donde se mostrará una lista de las carpetas que contienen las evidencias de ese control. Estas carpetas se organizan y nombran en función de la fecha en que se recopilaron las evidencias.
3. Elija el nombre de una carpeta de evidencias para abrirla. A continuación, revise un resumen de todas las evidencias reunidas en esa fecha. Este resumen incluye el número total de problemas de comprobación del cumplimiento que se notificaron directamente desde AWS Security Hub, AWS Config, o ambos. Para obtener instrucciones sobre cómo interpretar los datos de esta página, consulte Revisión de las carpetas de evidencias.
4. En la página de resumen de la carpeta de evidencias, navegue hasta la tabla de Evidencias. En la columna Tiempo, elija una partida para abrirla. Luego, revise los detalles sobre la prueba que se recopiló en ese momento. Para obtener instrucciones sobre cómo interpretar los datos de una página de detalles de las evidencias, consulte Revisión de las evidencias individuales.

> **Tip**
>
> Aunque AWS Audit Manager recopila automáticamente las evidencias para muchos controles, en algunos casos es posible que tenga que proporcionar evidencias adicionales para demostrar el cumplimiento. En estos casos, puede cargar las evidencias manualmente. Para obtener instrucciones, consulte Carga manual de evidencias.

Añadir un comentario a un control

Puede añadir comentarios a cualquier control que revise. El propietario de la auditoría puede ver estos comentarios.

Para añadir un comentario a un control

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija Notificaciones. O bien, seleccione Ver notificación en la barra flash azul situada en la parte superior de la pantalla para abrir la página de notificaciones.
3. En la página de Notificaciones, revise la lista de conjuntos de controles que se le han delegado. Busque el conjunto de controles que contiene el control para el que desea dejar un comentario y elija el nombre de la evaluación relacionada.
4. Seleccione la pestaña Controles, desplácese hacia abajo hasta la tabla de Conjuntos de controles y, a continuación, seleccione el nombre de un control para abrirlo.
5. Seleccione la pestaña Comentarios.
6. En Enviar comentarios, introduzca su comentario en el cuadro de texto.
7. Seleccione Enviar comentario para añadir su comentario. A continuación, su comentario aparece en la sección de Comentarios anteriores de la página, junto con cualquier otro comentario relacionado con este control.

Marcar un control como revisado

Puede indicar el progreso de la revisión actualizando el estado de los controles individuales de un conjunto de controles. Cambiar el estado del control es opcional. Sin embargo, le recomendamos que cambie el estado de cada control a Revisado a medida que complete la revisión de ese control.

Independientemente del estado de cada control individual, puede volver a enviar los controles al propietario de la auditoría.

Para marcar un control como revisado

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija Notificaciones. O bien, seleccione Ver notificación en la barra flash azul situada en la parte superior de la pantalla para abrir la página de notificaciones.
3. En la página de Notificaciones, revise la lista de conjuntos de controles que se le han delegado. Busque el conjunto de controles que desea marcar como revisado y elija el nombre de la evaluación relacionada.
4. En la pestaña Controles de la página de detalles de la evaluación, desplácese hacia abajo hasta la tabla de conjuntos de controles.
5. En la columna Controles agrupados por conjunto, expanda el nombre de un conjunto de controles para mostrar sus controles. Elija el nombre de un control para abrir la página de detalles del control.
6. Seleccione Actualizar el estado del control y cambie el estado a Revisado.
7. En la ventana emergente que aparece, seleccione Actualizar el estado del control para confirmar que ha terminado de revisar el control.

Volver a enviar el conjunto de controles revisado al propietario de la auditoría

Cuando haya terminado de revisar los controles que se le han delegado, envíe el conjunto de controles al propietario de la auditoría. Esto completa el proceso de delegación.

Para enviar un conjunto de control revisado al propietario de la auditoría

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija Notificaciones.
3. Revise la lista de conjuntos de controles que se le han delegado. Busque el conjunto de controles que desea devolver al propietario de la auditoría y elija el nombre de la evaluación relacionada.

4. Desplácese hacia abajo hasta la tabla de Conjunto de controles, seleccione el conjunto de controles que desee enviar al propietario de la auditoría y, a continuación, seleccione Enviar para su revisión.
5. En la ventana emergente que aparece, puede añadir comentarios antes de seleccionar Enviar para revisión. Una vez que envíe el control al propietario de la auditoría, este podrá ver cualquier comentario que le haya dejado.

Informes de evaluación

En un informe de evaluación se resumen las evidencias seleccionadas que se recopilaron para una evaluación. También contiene enlaces a archivos PDF con datos sobre cada evidencia. El contenido específico, la organización y la nomenclatura de un informe de evaluación dependen de los parámetros que elija al generar el informe.

Los informes de evaluación le ayudan a seleccionar y recopilar las evidencias pertinentes para su auditoría. Sin embargo, no evalúan la conformidad de las evidencias en sí. En su lugar, Audit Manager se limita a proporcionar los datos de la evidencia seleccionada como un resultado que puede compartir con su auditor.

Estructura de carpetas del informe de evaluación

Al descargar un informe de evaluación, Audit Manager genera una carpeta zip. Contiene su informe de evaluación y los archivos de evidencias relacionados en subcarpetas anidadas.

La carpeta zip se estructura como se indica a continuación:

- Carpeta de evaluación (ejemplo: `myAssessmentName-a1b2c3d4`): carpeta raíz.
  - Carpeta de informes de evaluación (ejemplo: `reportName-a1b2c3d4e5f6g7`): subcarpeta en la que se encuentran los archivos AssessmentReportSummary.pdf, digest.txt y README.txt.
    - Carpeta de evidencias por control (ejemplo: `controlName-a1b2c3d4e5f6g`): subcarpeta que agrupa los archivos de evidencias según el control relacionado.
      - Carpeta de evidencias por origen de datos (ejemplo: `CloudTrail`, `Security Hub`): subcarpeta que agrupa los archivos de evidencias por tipo de origen de datos.
        - Carpeta de evidencias por fecha (ejemplo: `2022-07-01`): subcarpeta que agrupa los archivos de evidencias por fecha de recopilación de evidencias.
          - Archivos de evidencias: archivos que contienen datos sobre las evidencias individuales.

¿Cómo navegar por un informe de evaluación?

Para empezar, abra la carpeta zip y baje un nivel hasta la carpeta del informe de evaluación. Aquí encontrará el informe de evaluación en PDF y el archivo README.txt.

Puede revisar el archivo README.txt para comprender la estructura y el contenido de la carpeta zip. También proporciona información de referencia sobre las convenciones de nomenclatura de cada archivo. Esta información puede ayudarle a navegar directamente a una subcarpeta o a un archivo de evidencias si está buscando un elemento específico.

De lo contrario, para buscar evidencias y encontrar la información que necesita, abra el PDF del informe de evaluación. Esto le proporciona una visión general de alto nivel del informe y un resumen de la evaluación a partir de la cual se creó el informe.

A continuación, utilice el índice (TOC) para explorar el informe. Puede elegir cualquier control hipervinculado del índice para ir directamente a un resumen de ese control.

Cuando esté listo para revisar los datos de las evidencias de un control, puede hacerlo eligiendo el nombre de la evidencia con hipervínculos. En el caso de las evidencias automatizadas, el hipervínculo abre un nuevo archivo PDF con datos sobre esas evidencias. En el caso de las evidencias manuales, el hipervínculo lleva al bucket de S3 que contiene las evidencias.

> **Tip**
>
> La ruta de navegación situada en la parte superior de cada página muestra su ubicación actual en el informe de evaluación a medida que examina los controles y las evidencias. Seleccione el índice con el hiperenlace para volver al índice en cualquier momento.

Secciones del informe de evaluación

Utilice la siguiente información para obtener más datos sobre cada sección de un informe de evaluación.

> **Note**
>
> Si ve un guion (-) junto a cualquiera de los atributos de las siguientes secciones, esto indica que el valor de ese atributo es nulo o que no existe ningún valor.

- Portada
- Página de información general
- Página del índice

- Página de control
- Página de resumen de evidencias
- Página de información sobre evidencias

Portada

La portada incluye el nombre del informe de evaluación. También muestra la fecha y la hora en que se generó el informe, junto con el ID de cuenta del usuario que lo generó.

La portada tiene el siguiente formato. Audit Manager reemplaza los *marcadores de posición* por la información pertinente para su informe.

```
Assessment report name
Report generated on MM/DD/YYYY at HH:MM:SS AM/PM UCT by AccountID
```

Página de información general

La página de información general consta de dos partes: un resumen del informe en sí y un resumen de la evaluación sobre la que se informa.

Resumen de informe

En esta sección se resume el informe de evaluación.

- Nombre del informe: el nombre del informe.
- Descripción: descripción que introduce el propietario de la auditoría al generar el informe.
- Fecha de generación: fecha en que se generó el informe. La hora se representa en formato de hora universal coordinada (UTC).
- Total de controles incluidos: número de controles que se incluyen en el informe y que han recopilado evidencias. Se trata de un subconjunto del número total de controles de la evaluación.
- Cuentas de AWS incluidas: el número de Cuentas de AWS que se incluyen en el informe y que han recopilado evidencias. Se trata de un subconjunto del número total de Cuentas de AWS de la evaluación.
- Selección del informe de evaluación: número de elementos de evidencia que se seleccionan para su inclusión en el informe. Incluye el número total de problemas de control de la conformidad incluidos en el informe.

Resumen de la evaluación

Esta sección resume la evaluación a la que se refiere el informe.

- Nombre de la evaluación: nombre de la evaluación a partir de la cual se generó el informe.
- Estado: estado de la evaluación en el momento en que se generó el informe.
- Región de evaluación: la Región de AWS en la que se creó la evaluación.
- Cuentas de AWS en el ámbito: lista completa de Cuentas de AWS incluidas en el ámbito de la evaluación.
- Servicios de AWS en el ámbito: lista completa de Servicios de AWS incluidos en el ámbito de la evaluación.
- Nombre del marco: nombre del marco a partir del cual se creó la evaluación.
- Propietarios de la auditoría: usuario o rol de los propietarios de la auditoría de la evaluación.
- Última actualización: fecha en la que se actualizó por última vez la evaluación. La hora se representa en UTC.

Página del índice

En el índice se muestra el contenido completo del informe de evaluación. El contenido se agrupa y organiza en función de los conjuntos de control que se incluyen en la evaluación. Los controles se enumeran debajo de su conjunto de controles respectivo.

Seleccione cualquier elemento del índice para ir directamente a esa sección del informe. Puede elegir un conjunto de controles o ir directamente a un control.

Página de control

La página de control consta de dos partes: un resumen del control en sí y un resumen de las evidencias recopiladas para el control.

Resumen de control

Esta sección incluye la siguiente información.

- Nombre de control: el nombre del control.
- Descripción: la descripción del control.

- Conjunto de controles: nombre del conjunto de controles al que pertenece el control.
- Información de prueba: los procedimientos de prueba recomendados para este control.
- Plan de acción: acciones recomendadas para realizar si no se cumple el control.
- Selección del informe de evaluación: número de elementos de evidencia relacionados con este control incluidos en el informe de evaluación. Esto incluye el número de problemas de verificación de conformidad que se detectaron en las evidencias de este control.

Evidencia recopilada

En esta sección se muestran las evidencias recopiladas para el control. Las evidencias se agrupan en carpetas, que se organizan y nombran según la fecha de recolección de las mismas. Junto al nombre de cada carpeta de evidencias aparece el número total de problemas de verificación de conformidad relacionados con esa carpeta.

Debajo del nombre de cada carpeta de evidencias hay una lista de nombres de evidencias con hipervínculos.

- Los nombres de las evidencias automatizadas comienzan con una marca de tiempo de recopilación de evidencias, seguida del código de servicio, el nombre del evento (hasta 20 caracteres), el identificador de la cuenta y un identificador único de 12 caracteres.

  Por ejemplo: `21-30-24_IAM_CreateUser_111122223333_a1b2c3d4e5f6`

  En el caso de las evidencias automatizadas, el nombre del hipervínculo abre un nuevo archivo PDF con un resumen y más información.
- Los nombres de las evidencias manuales comienzan con una marca de tiempo de carga de las evidencias, seguida de la etiqueta `manual`, el identificador de cuenta y un identificador único de 12 caracteres. También incluyen los 10 primeros caracteres del nombre del archivo y la extensión del archivo (hasta 10 caracteres).

  Por ejemplo: `00-00-00_manual_111122223333_a1b2c3d4e5f6_myimage.png`

  Para evidencia manual, el nombre del hipervínculo lo lleva al bucket de S3 que contiene esa evidencia.

Junto al nombre de cada evidencia aparece el resultado de la comprobación de conformidad de ese elemento.

- En el caso de las evidencias automatizadas recopiladas de AWS Security Hub o AWS Config, se informa de un resultado Conforme, No conforme o No concluyente.
- En el caso de las evidencias automatizadas recopiladas a partir de las llamadas a la API y AWS CloudTrail, y de todas las evidencias manuales, se muestra un resultado de No concluyente.

Página de resumen de evidencias

La página de resumen de evidencias incluye la siguiente información:

- ID: identificador único de la evidencia.
- Fecha de recopilación: fecha en que se creó o cargó la evidencia.
- Descripción: descripción de las evidencias, incluidos el identificador de la cuenta y el tipo de origen de datos.
- Nombre de la evaluación: nombre de la evaluación a partir de la cual se generó el informe.
- Nombre del marco: nombre del marco a partir del cual se creó la evaluación.
- Nombre del control: nombre del control que respaldan las evidencias.
- Nombre del conjunto de controles: nombre del conjunto de controles al que pertenece el control relacionado.
- Descripción del control: descripción del control que respaldan las evidencias.
- Información de prueba: los procedimientos de prueba recomendados para el control.
- Plan de acción: las acciones recomendadas para realizar si no se cumple el control.
- Región de AWS: el nombre de la región asociada con la evidencia.
- ID de IAM: ARN del usuario o rol asociado a la evidencia.
- Cuenta de AWS: identificador de Cuenta de AWS asociado a la evidencia.
- Servicio de AWS: el nombre del Servicio de AWS asociado con la evidencia.
- Recursos incluidos: recursos de AWS evaluados para generar la evidencia. Este atributo no se aplica a las evidencias de verificación de conformidad de AWS Config. Para este tipo de evidencias, puede encontrar todos los recursos tabulados en el Página de información sobre evidencias del PDF de evidencias.
- Nombre del evento: nombre del evento de evidencias.
- Tiempo de eventos: la hora de cuando se produjo el evento de evidencia.
- Origen de datos: lugar desde el que se recopilaron o cargaron las evidencias. El origen de datos puede ser AWS Config, centro de seguridad, llamadas a AWS API, CloudTrail o manual.

- Evidencia por tipo: categoría de la evidencia
  - Las evidencias de verificación de conformidad se recopilan en AWS Config o en nuestro centro de seguridad.
  - Las evidencias relativas a la actividad del usuario se recopilan en los registros de CloudTrail.
  - Las evidencias relativas a los datos de configuración se recopilan a partir de instantáneas de otros Servicios de AWS.
  - Las evidencias manuales son aquellas que se cargan manualmente.
- Estado de la verificación de conformidad: estado de la evaluación de las evidencias incluidas en la categoría de verificación de conformidad.
  - En el caso de las evidencias automatizadas recopiladas de AWS Security Hub o AWS Config, se informa de un resultado Conforme, No conforme o No concluyente.
  - En el caso de las evidencias automatizadas recopiladas a partir de las llamadas a la API y AWS CloudTrail, y de todas las evidencias manuales, se muestra un resultado de No concluyente.

Página de información sobre evidencias

En la página de información sobre evidencias aparece el nombre de la evidencia y una tabla de datos de la misma. En esta tabla se proporciona un desglose detallado de cada elemento de la evidencia para que pueda entender los datos y validar que son correctos. Según el origen de datos de las evidencias, el contenido de la página de información sobre las evidencias variará.

> **Tip**
>
> La ruta de navegación en la parte superior de cada página muestra su ubicación actual a medida que explora los detalles de las evidencias. Seleccione Resumen de evidencias para volver al resumen de evidencias en cualquier momento.

Verificación de la integridad del informe de evaluación

Al generar un informe de evaluación, Audit Manager genera una suma de comprobación del archivo de informe denominada `digest.txt`. Puede utilizar este archivo para validar la integridad del informe y asegurarse de que no se modificó ninguna evidencia después de la creación del informe. Contiene un objeto JSON con firmas y códigos hash que se invalidan si se modifica alguna parte del archivo del informe.

Para validar la integridad de un informe de evaluación, utilice la API ValidateAssessmentReportIntegrity proporcionada por Audit Manager.

Informes de evaluación de solución de problemas

Para encontrar respuestas a preguntas y problemas comunes, consulte Solución de problemas del informe de evaluación en la sección Solución de problemas de esta guía.

Buscador de evidencias

El buscador de evidencias proporciona una forma eficaz de buscar evidencias en Audit Manager. En lugar de explorar exhaustivamente carpetas de evidencias para encontrar lo que busca, ahora puede utilizar el buscador de evidencias para consultarlas rápidamente. Si utiliza el buscador de evidencias como administrador delegado, puede buscar evidencias en todas las cuentas de miembros de su organización.

Mediante una combinación de filtros y agrupaciones, puede reducir progresivamente el alcance de su consulta de búsqueda. Por ejemplo, si desea obtener una visión general del estado de su sistema, realice una búsqueda amplia y filtre por evaluación, intervalo de fechas y conformidad de los recursos. Si su objetivo es corregir un recurso específico, puede realizar una búsqueda restringida para encontrar evidencias que apunten a un identificador de control o recurso específico. Tras definir los filtros, puede agrupar y, a continuación, obtener una vista previa de los resultados de búsqueda coincidentes antes de crear un informe de evaluación.

Para utilizar el buscador de evidencias, debe habilitar esta característica en la configuración de Audit Manager.

Temas

Comprender cómo funciona el buscador de evidencias con CloudTrail Lake

El buscador de evidencias utiliza la capacidad de consulta y almacenamiento de AWS CloudTrail Lake. Antes de empezar a utilizar el buscador de evidencias, es útil entender un poco más sobre el funcionamiento de CloudTrail Lake.

CloudTrail Lake añade datos en un único almacén de datos de eventos con capacidad de búsqueda que admite consultas SQL de gran alcance. Esto significa que puede buscar datos en toda su organización y dentro de intervalos de tiempo personalizados. Con el buscador de evidencias, puede utilizar esta función de búsqueda directamente en la consola de Audit Manager.

Cuando solicita habilitar el buscador de evidencias, Audit Manager crea un almacén de datos de eventos en su nombre. Una vez habilitado el buscador de evidencias, todas las evidencias futuras de Audit Manager se incorporarán al almacén de datos del evento, donde estarán disponibles para las consultas de búsqueda del buscador de evidencias. Después de habilitar el buscador de evidencias, también rellenamos el almacén de datos de eventos recién creado con los datos de evidencias de los dos últimos años. Si habilita el buscador de evidencias como administrador delegado, rellenaremos los datos de todas las cuentas de los miembros de la organización.

Todas sus evidencias, ya sean nuevas o repuestas, se retienen en el almacén de datos de evidencias durante 2 años. Puede cambiar el periodo de retención predeterminado en cualquier momento. Para obtener instrucciones, consulte Actualizar un almacén de datos de eventos en la Guía del usuario de AWS CloudTrail. Puede conservar datos de eventos en un almacén de datos de eventos por hasta 7 años o 2555 días.

> **Note**
>
> El proceso de cumplimentación de datos, cuando esta característica está habilitada, es gratuito si se realiza antes de noviembre de 2023.
> Cuando se añadan nuevos datos de evidencias al almacén de datos del evento en el futuro, se incurrirá en cargos de CloudTrail Lake por la incorporación y almacenamiento de datos.
> Las consultas de CloudTrail Lake son de pago por uso. Esto significa que, por cada consulta de búsqueda que ejecute en el buscador de evidencias, se le cobrará por los datos escaneados.
> Para obtener más información sobre los precios de CloudTrail Lake, consulte Precios de AWS CloudTrail.

Habilitar el buscador de evidencias

Puede habilitar el buscador de evidencias en la configuración de Audit Manager. Para obtener instrucciones, consulte Buscador de evidencias en la página Configuración de AWS Audit Manager de esta guía.

Solución de problemas del buscador de evidencias

Para encontrar respuestas a preguntas y problemas comunes, consulte Solución de problemas relacionados con la búsqueda de evidencias en la sección Solución de problemas de esta guía.

Buscar evidencias

Siga estos pasos para buscar evidencias en la consola de Audit Manager.

> **Note**
>
> También puede utilizar la API de CloudTrail para consultar los datos de las evidencias. Para obtener más información, consulte StartQuery en la Referencia de la API de AWS CloudTrail. Si prefiere utilizar la AWS CLI, consulte Iniciar una consulta en la Guía del usuario de AWS CloudTrail.

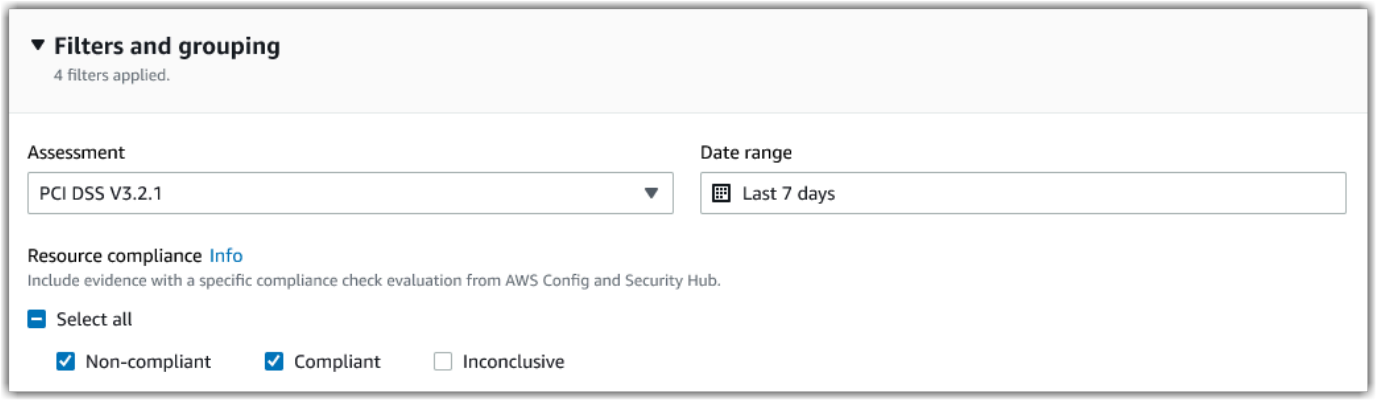
En esta página

Realizar una consulta de búsqueda

Siga estos pasos para realizar una consulta de búsqueda en el buscador de evidencias.

Para buscar evidencias

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, seleccione Buscador de evidencias.
3. A continuación, aplique filtros para limitar el alcance de la búsqueda.
    a. En Evaluación, elija una evaluación.
    b. En Intervalo de fechas, seleccione un intervalo.
    c. En Conformidad de los recursos, seleccione un estado de evaluación.

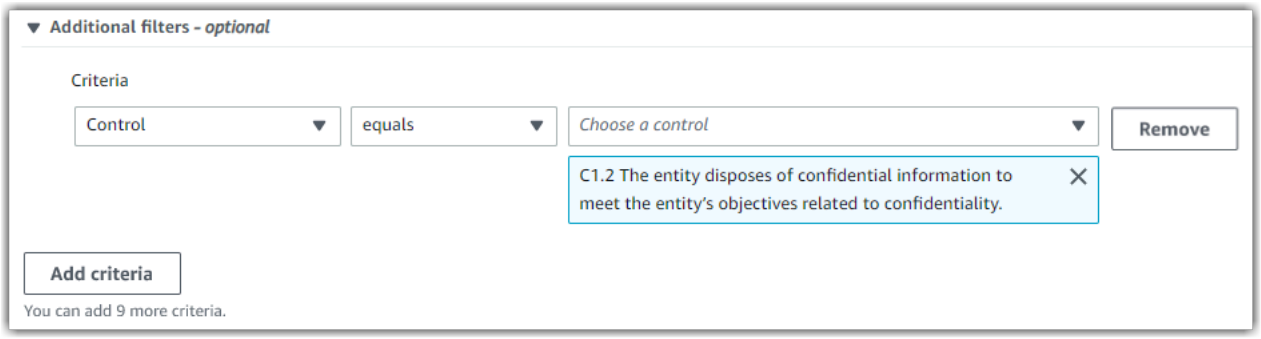


4. (Opcional) Seleccione filtros adicionales (opcionales) para restringir aún más la búsqueda.

   a. Seleccione Añadir criterios, seleccione un criterio y, a continuación, seleccione uno o más valores para ese criterio.

   b. Siga creando más filtros de la misma manera.

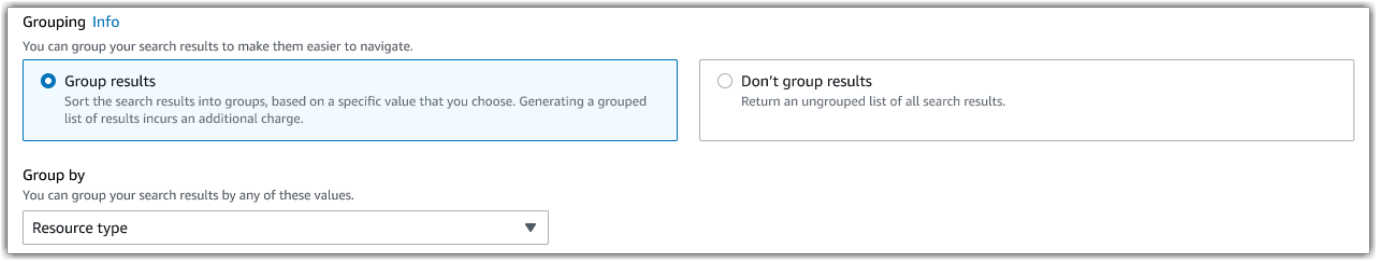
   c. Para eliminar un filtro no deseado, seleccione Eliminar.



5. En Agrupación, especifique si desea agrupar los resultados de la búsqueda.

   a. Si desea agrupar los resultados, seleccione un valor por el que agruparlos.

   b. Si no desea agrupar los resultados, continúe con el paso 6.



6. Elija Search (Buscar).

La búsqueda puede tardar unos minutos, en función de la cantidad de datos de evidencias de los que disponga. Puede salir del buscador de evidencias mientras la búsqueda está en curso. Una barra parpadeante le avisará cuando los resultados de la búsqueda estén listos.

> **Tip**
>
> Para obtener más información sobre los filtros y agrupaciones que puede usar en este procedimiento, consulte Opciones de filtrado y agrupamiento.

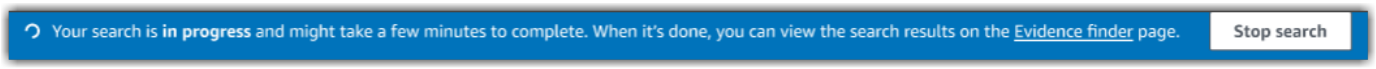
Detener una consulta de búsqueda

Si desea detener una consulta de búsqueda por cualquier motivo, siga estos pasos.

> **Note**
>
> Detener una consulta de búsqueda aún puede generar cargos. Se le cobrará la cantidad de datos de evidencias escaneados antes de detener la consulta de búsqueda. Cuando se detenga, podrá ver los resultados parciales devueltos.

Para detener una consulta de búsqueda en curso

1. En la barra parpadeante de progreso azul de la parte superior de la pantalla, seleccione Detener búsqueda.



2. (Opcional) Revise los resultados parciales devueltos antes de detener la consulta de búsqueda.
   a. Si se encuentra en la página del buscador de evidencias, los resultados parciales se muestran en la pantalla.
   b. Si ha navegado fuera del buscador de evidencias, seleccione Ver resultados parciales en la barra parpadeante de confirmación verde.

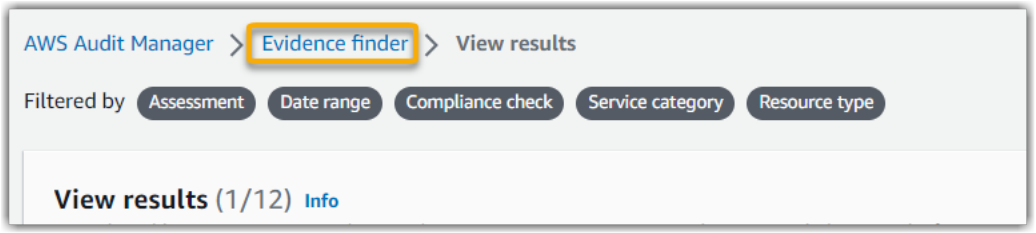
Editar filtros de búsqueda

Puede volver a la consulta de búsqueda más reciente y cambiar los filtros según sea necesario.

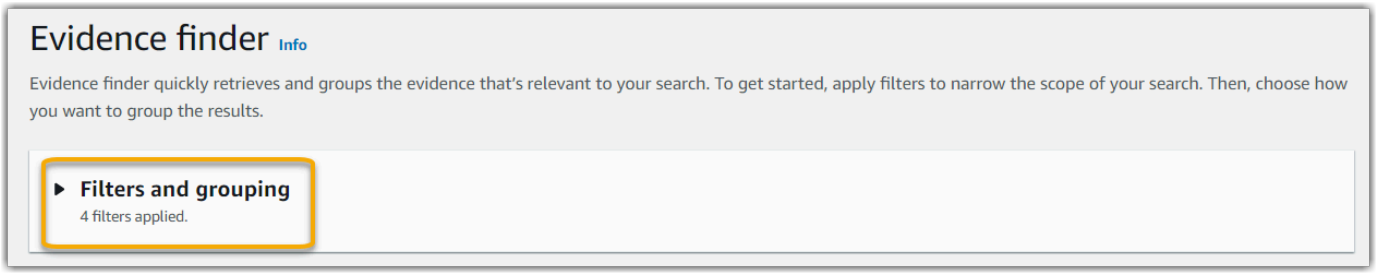
> **Note**
>
> Al editar los filtros y seleccionar Buscar, se inicia una nueva consulta de búsqueda.

Para editar una consulta de búsqueda reciente

1. En la página Ver resultados, seleccione Buscador de evidencias en el menú de navegación de la ruta de navegación.



2. Seleccione Filtros y agrupaciones para ampliar la selección de filtros.



3. A continuación, edite sus filtros o inicie una nueva búsqueda.

   a. Para editar los filtros, ajuste o elimine los filtros actuales y la selección de agrupación.

   b. Para volver a empezar, seleccione Borrar filtros y aplique los filtros y agrupaciones que prefiera.

4. Cuando haya terminado, elija Buscar.

Visualizar los resultados en el buscador de evidencias

Una vez finalizada la búsqueda, podrá ver los resultados que coincidan con sus criterios de búsqueda.

Tenga en cuenta que es posible que se evalúen varios recursos durante la recopilación de evidencias. Como resultado, la evidencia puede incluir uno o varios recursos relacionados. En el buscador de evidencias, los resultados se muestran a nivel de recurso, con una fila para cada recurso. Puede previsualizar un resumen de cada recurso sin salir de la página.

Tras revisar los resultados de la búsqueda, puede generar un informe de evaluación que incluya esas evidencias. También puede exportar los resultados de la búsqueda a un archivo de valores separados por comas (CSV).

> **Important**
>
> Le recomendamos que mantenga abierto el buscador de evidencias hasta que termine de explorar los resultados de la búsqueda. Los resultados de la búsqueda se descartan al salir de la tabla Ver resultados. Si es necesario, puede ver los resultados recientes en la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/. Aquí, los resultados de sus consultas de búsqueda se guardan durante siete días. Sin embargo, tenga en cuenta que no puede generar un informe de evaluación a partir de los resultados de búsqueda en la consola de CloudTrail.

En esta página

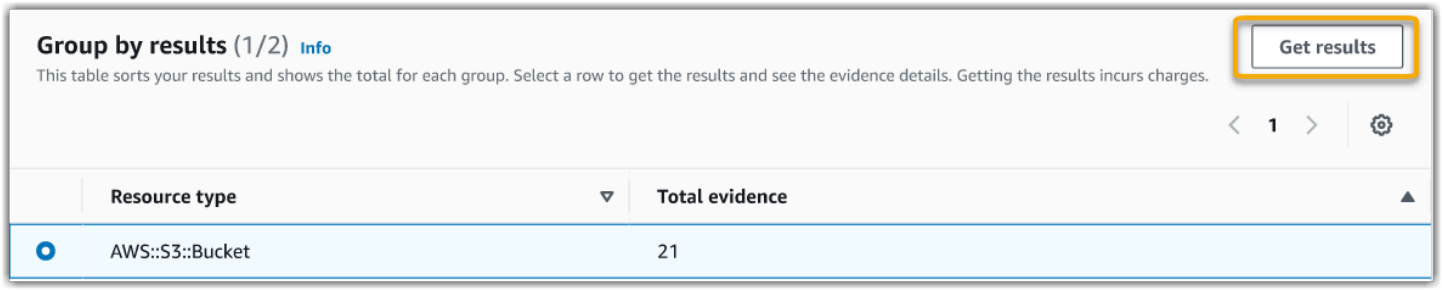
- Administrar sus preferencias de visualización
- Vista previa de resúmenes de recursos
- Genere un informe de evaluación a partir de los resultados de su búsqueda
- Exporte los resultados de búsqueda

Visualizar resultados agrupados

Si agrupó los resultados, puede revisarlos antes de examinar las evidencias.

> **Note**
>
> Si no agrupó los resultados, el buscador de evidencias no mostrará la tabla Agrupar por resultados. En su lugar, accederá directamente a la tabla Ver resultados.

Utilice la tabla Agrupar por resultados para conocer el alcance de la evidencia coincidente y cómo se distribuye en una dimensión específica. Los resultados se agrupan según el valor que haya seleccionado. Por ejemplo, si los ha agrupado por tipo de recurso, en la tabla se mostrará una lista de los tipos de recursos de AWS. En la columna de Evidencia total se mostrará el número de resultados coincidentes para cada tipo de recurso.



Para obtener los resultados de un grupo

1. En la tabla Agrupar por resultados, seleccione la fila de los resultados que desee obtener.
2. Seleccione Obtener resultados. Esto iniciará una nueva consulta de búsqueda y le redirigirá a la tabla Ver resultados, donde podrá ver los resultados de ese grupo.

Visualización de los resultados de búsqueda

En la tabla Ver resultados se muestran los resultados de la búsqueda. Desde aquí puede realizar las siguientes acciones:

- Administrar sus preferencias de visualización
- Vista previa de resúmenes de recursos
- Genere un informe de evaluación a partir de los resultados de su búsqueda
- Exporte los resultados de búsqueda

Administrar sus preferencias de visualización

Sus preferencias de visualización controlan lo que ve en la página de resultados.

Administrar sus preferencias de visualización

1. Seleccione el icono de configuración (#) situado en la parte superior de la tabla Ver resultados.
2. Revise y cambie la configuración siguiente como sea necesario:
    a. Seleccionar columnas visibles de la tabla: utilice la opción de alternancia para cambiar las columnas que se muestran.
    b. Tamaño de página: seleccione un botón de opción para especificar cuántos resultados se muestran en cada página.
    c. Ajustar texto: marque la casilla de verificación para ajustar líneas de texto largas y mejorar la legibilidad.
3. Elija Confirmar para guardar las preferencias.

Vista previa de resúmenes de recursos

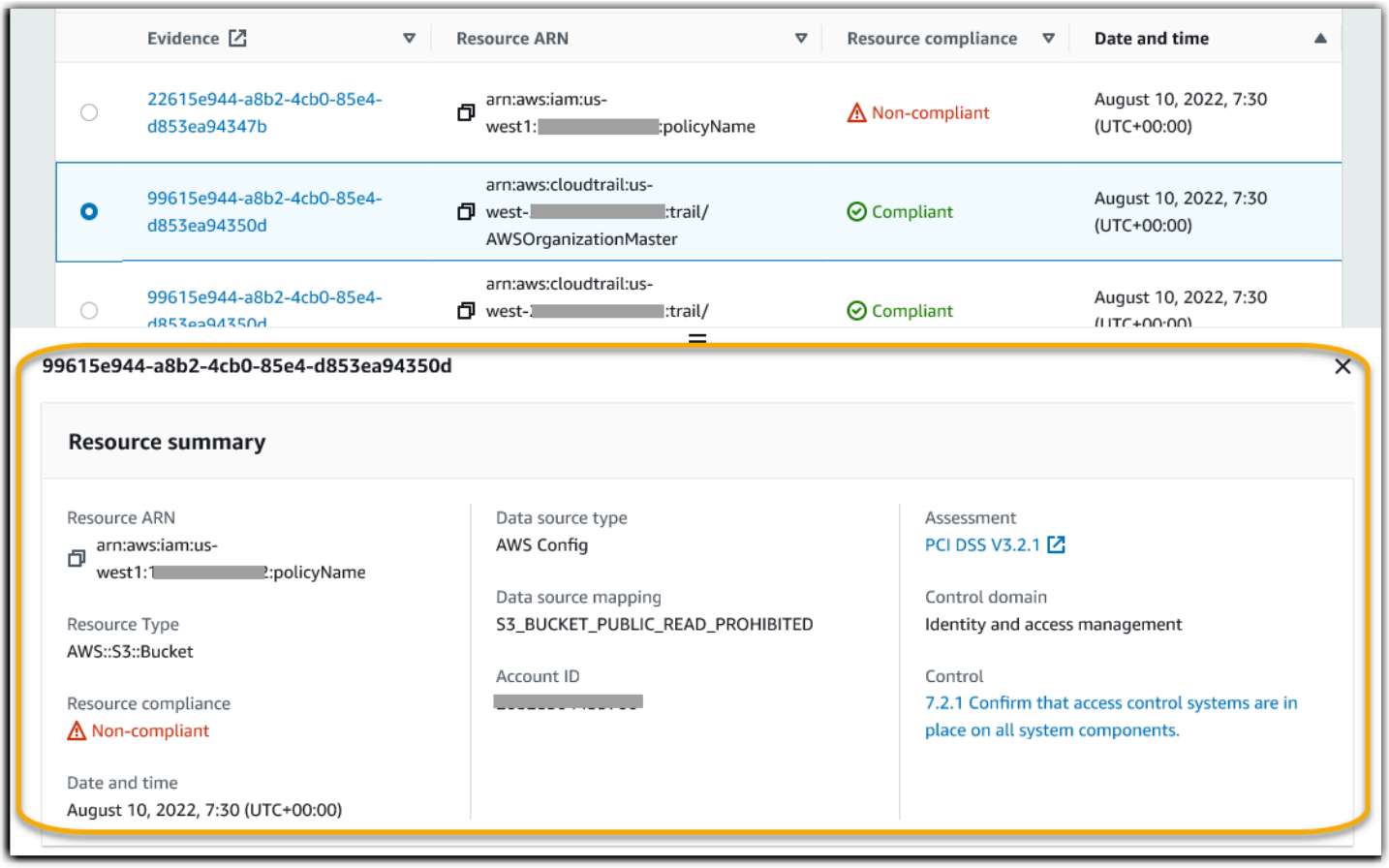
Puede obtener una vista previa de los recursos relacionados con las evidencias que coincidan con su consulta de búsqueda. Esto le ayuda a determinar si la consulta de búsqueda arrojó los resultados esperados o si necesita ajustar los filtros y volver a ejecutar la consulta de búsqueda.

Tenga en cuenta que las evidencias pueden tener uno o más recursos relacionados. El buscador de evidencias muestra los resultados a nivel de recurso (con una fila para cada recurso).

> **Note**
>
> El buscador de evidencias devuelve los resultados de las evidencias automatizadas y manuales. Sin embargo, solo puede obtener vista previa de resúmenes de recursos para evidencias automatizadas. Esto se debe a que Audit Manager no realiza evaluaciones de recursos para obtener evidencias manuales y, como resultado, no hay un resumen de recursos disponibles.
>
> Para consultar los datos sobre la evidencia manual, seleccione el nombre de la evidencia para abrir la página de datos de la evidencia. Si genera un informe de evaluación a partir de los resultados del buscador de evidencias, los datos de las evidencias manuales se incluyen en el informe de evaluación.

Vista previa de resúmenes de recursos

1. Seleccione el botón de opción situado junto al resultado. Se abrirá un panel de resumen de recursos en la página actual.
2. (Opcional) Para ver todos los datos de la evidencia relacionada, seleccione el nombre de la evidencia.
3. (Opcional) Utilice las líneas horizontales (=) para arrastrar y cambiar el tamaño del panel de resumen de recursos.
4. Seleccione (x) para cerrar el panel de resumen de recursos.



Genere un informe de evaluación a partir de los resultados de su búsqueda

Una vez que esté satisfecho con los resultados de la búsqueda, genere un informe de evaluación.

Genere un informe de evaluación a partir de los resultados de la búsqueda

1. En la parte superior de la tabla Ver resultados, seleccione Generar informe de evaluación.
2. Introduzca un nombre y una descripción para el informe de evaluación y revise los detalles del informe de evaluación.
3. Seleccione Generar informe de evaluación.

Se tarda unos minutos en generar el informe de evaluación. Mientras tanto, puede salir del buscador de evidencias. Aparecerá una notificación de éxito de color verde que confirmará que el informe está listo. A continuación, puede ir al centro de descargas de Audit Manager y descargar su informe de evaluación.

> **Note**
>
> Audit Manager generará un informe único utilizando únicamente la evidencia de los resultados de la búsqueda. Este informe no incluye ninguna evidencia que se haya agregado manualmente a un informe desde la página de evaluación.
> Existen límites a la cantidad de evidencias que se pueden incluir en un informe de evaluación. Para obtener más información, consulte Solución de problemas del buscador de evidencias.

Exporte los resultados de búsqueda

Es posible que necesite una versión portátil de los resultados de búsqueda de su buscador de evidencias. De ser así, puede exportar los resultados de la búsqueda a un archivo CSV.

Tras exportar los resultados de la búsqueda, el archivo CSV estará disponible en el centro de descargas de Audit Manager durante siete días. También se envía una copia del archivo CSV a su bucket de S3 preferido, que se conoce como destino de exportación. El archivo CSV permanece disponible en este bucket hasta que lo elimine.

Audit Manager utiliza la funcionalidad de CloudTrail Lake para exportar y entregar archivos CSV desde el buscador de evidencias. Los siguientes factores definen cómo funciona el proceso de exportación de CSV:

- Todos los resultados de la búsqueda se incluyen en el archivo CSV. Si solo quiere incluir resultados de búsqueda específicos, le recomendamos que edite sus filtros de búsqueda. De esta forma, puede restringir los resultados para orientarlos únicamente a las evidencias que desee exportar.
- Los archivos CSV se exportan en formato GZIP comprimido. El nombre predeterminado del archivo CSV es `queryID/result.csv.gz`, donde `queryID` es el ID de la consulta de búsqueda.
- El tamaño de archivo máximo de una exportación CSV es de 1 TB. Si exporta más de 1 TB de datos, los resultados se dividirán en más de un archivo. Cada archivo CSV se denomina `result_`*`number`*`.csv.gz`. La cantidad de archivos CSV que reciba dependerá del tamaño total de los resultados de la búsqueda. Por ejemplo, al exportar 2 TB de datos se obtendrán dos archivos de resultados de consultas: `result_1.csv.gz` `yresult_2.csv.gz`.
- Además del archivo CSV, se enviará un archivo de firma JSON a su bucket de S3. Este archivo actuará como una suma de comprobación para verificar que la información del archivo CSV

es correcta. Para obtener más información, consulte Estructura de archivos de señalización de CloudTrail en la Guía para desarrolladores de AWS CloudTrail. Para determinar si los resultados de la consulta se han modificado, eliminado o continúan igual después del envío, puede usar la validación de integridad de los resultados de las consultas de CloudTrail. Para obtener instrucciones, consulte Validar los resultados de las consultas guardadas en la Guía para desarrolladores de AWS CloudTrail.

> **Note**
>
> Las respuestas textuales de evidencias manuales no se incluyen actualmente en las vistas previas del buscador de evidencias ni en las exportaciones a CSV. Para ver los datos de la respuesta textual, seleccione el nombre de la evidencia manual en el buscador de resultados para abrir la página de detalles de la evidencia. Si necesita ver los datos de las respuestas de texto fuera de la consola de Audit Manager, le recomendamos que genere un informe de evaluación a partir de los resultados del buscador de evidencias. Todos los datos de las evidencias manuales, incluidas las respuestas en texto, se incluyen en los informes de evaluación.

Exportar resultados por primera vez

Siga estos pasos para exportar los resultados de búsqueda por primera vez. Este procedimiento le da la opción de especificar un destino de exportación predeterminado para todas sus futuras exportaciones. Si no desea guardar un destino de exportación predeterminado en este momento, puede hacerlo más adelante actualizando la configuración del destino de exportación.

> **Important**
>
> Antes de empezar, asegúrese de tener un bucket de S3 disponible para usarlo como destino de exportación. Puede usar uno de sus buckets de S3 existentes o puede crear uno nuevo en Amazon S3. El bucket de S3 debe tener la política de permisos requerida para permitir que CloudTrail escriba los archivos de exportación en él. Más específicamente, la política de buckets debe incluir una acción `s3:PutObject` y el ARN del bucket, además de incluir CloudTrail como entidad principal del servicio. Proporcionamos un ejemplo de política de permisos que puede utilizar. Para obtener instrucciones sobre cómo adjuntar esta política a su bucket de S3, consulte Añadir una política de buckets mediante la consola de Amazon S3.

Para obtener más consejos, consulte los Consejos de configuración para su destino de exportación. Si tiene algún problema al exportar un archivo CSV, consulte Solución de problemas de las exportaciones a CSV del buscador de evidencias.

Para exportar los resultados de la búsqueda (primera ejecución)

1. En la parte superior de la tabla Ver resultados, seleccione Exportar CSV.
2. Especifique el bucket de S3 al que desea exportar su archivo.
   - Seleccione Explorar S3 para elegir de una lista de sus buckets.
   - Como alternativa, puede introducir el URI del bucket en este formato: **`s3://bucketname/prefix`**

   > **Tip**
   >
   > Para mantener el bucket de destino organizado, puede crear una carpeta opcional para sus exportaciones a CSV. Para ello, añada una barra (**`/`**) y un prefijo al valor del cuadro URI del recurso (por ejemplo, **`/evidenceFinderExports`**). A continuación, Audit Manager incluirá este prefijo cuando añada el archivo CSV al bucket y Amazon S3 generará la ruta especificada por el prefijo. Para obtener más información acerca de los prefijos en Amazon S3, consulte Organizar objetos en la consola de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.
3. (Opcional) Si no quiere guardar este bucket como destino de exportación predeterminado, desmarque la casilla de verificación que indica Guardar este bucket como destino de exportación predeterminado en la configuración de mi buscador de evidencias.
4. Elija Export (Exportar).

Exportar los resultados después de guardar un destino de exportación

Una vez que haya guardado un bucket de S3 predeterminado como destino de exportación predeterminado, puede seguir estos pasos en el futuro.

Para exportar los resultados de la búsqueda (después de guardar un destino de exportación predeterminado)

1. En la parte superior de la tabla Ver resultados, seleccione Exportar CSV.
2. En el mensaje que aparece, revise el bucket de S3 predeterminado en el que se guardará el archivo exportado.

   a. (Opcional) Para seguir usando este bucket y ocultar este mensaje en el futuro, marque la casilla No volver a recordármelo.

   b. (Opcional) Para cambiar este bucket, siga el procedimiento para actualizar la configuración del destino de exportación.
3. Elija Confirmar.

Según la cantidad de datos que exporte, el proceso de exportación puede tardar unos minutos en completarse. Puede navegar fuera del buscador de evidencias mientras la exportación está en curso. Al salir del buscador de evidencias, la búsqueda se detendrá y los resultados de la búsqueda se descartarán en la consola. Sin embargo, el proceso de exportación a CSV continuará en segundo plano. El archivo CSV contendrá el conjunto completo de resultados de búsqueda que coincidan con su consulta.

Ver los resultados después de exportarlos

Para buscar su archivo CSV y comprobar su estado, vaya al centro de descargas de Audit Manager. Cuando el archivo exportado esté listo, puede descargar su archivo CSV desde el centro de descargas.

También puede buscar y descargar el archivo CSV desde el bucket de S3 de destino de exportación.

Para buscar el archivo CSV y el archivo de firma en la consola de Amazon S3

1. Abra la consola de Amazon S3.
2. Seleccione el bucket de destino de exportación que especificó al exportar el archivo CSV.
3. Recorra la jerarquía de objetos hasta que encuentre el archivo CSV y el archivo de firma. El archivo CSV tiene una extensión `.csv.gz` y el archivo de firma tiene una extensión `.json`.

Verá una jerarquía de objetos similar a la del siguiente ejemplo, pero con diferente nombre de bucket para el destino de exportación, ID de cuenta, fecha e ID de consulta.

```
All Buckets
    Export_Destination_Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        YYYY
                            MM
                              DD
                                Query_ID
```

Opciones de filtros y agrupaciones

En esta página se describen las opciones de filtrado y agrupación disponibles en el buscador de evidencias.

En esta página

Referencia de filtro

Puede utilizar los siguientes filtros para buscar evidencias que coincidan con criterios específicos, como una evaluación, un control o Servicio de AWS.

Temas

filtros requeridos

Utilice estos filtros para comenzar con información general de alto nivel de la evidencia de una evaluación.

Nombre del filtro	Descripción	Notas
Evaluación	Devuelve la evidencia de una evaluación específica.	Puede filtrar por una sola evaluación.
Rango de fechas	Devuelve evidencia de un periodo de tiempo específico.	O bien, puede usar un Rango relativo para definir un rango relativo a la fecha de hoy (por ejemplo, **`Last 30 days`**). O bien, puede usar un Rango absoluto para especificar un rango de fechas específico (por ejemplo, **`June 27th - July 4th`**).
Conformidad de recursos	Devuelve los recursos con una evaluación de verificación de conformidad específica.	Audit Manager recopila evidencias de verificación de conformidad para los controles que utilizan AWS Config y Security Hub como tipo de origen de datos. Es posible que se evalúen varios recursos durante la recopilación de evidencias. En consecuencia, una sola prueba de verificación de conformidad puede incluir uno o más recursos. Puede usar este filtro para explorar el estado de conformidad a nivel de recurso. Puede elegir una o más de las siguientes opciones: • No conformidad: este filtro encuentra recursos con problemas de verificación de conformidad. Este es el caso si Security Hub informa de un resultado Fallido o AWS Config informa de un resultado de no conformidad. • Conformidad: este filtro encuentra recursos sin problemas de verificación de conformidad. Esto sucede si Security Hub informa de un resultado Aprobado o si AWS Config informa de un resultado de Conformidad.

Nombre del filtro	Descripción	Notas
		• No concluyente: este filtro busca recursos para los que no haya una verificación de conformidad disponible o aplicable. Esto ocurre si un recurso utiliza AWS Config o Security Hub como tipo de origen de datos subyacente, pero esos servicios no están habilitados. Esto también ocurre si el recurso utiliza un tipo de origen de datos subyacente que no admita las comprobaciones de conformidad (como las evidencias manuales, las llamadas a la AWS API o CloudTrail).

Filtros adicionales (opcionales)

Utilice estos filtros para limitar el alcance de la consulta de búsqueda. Por ejemplo, utilice Servicio para ver todas las evidencias relacionadas con Amazon S3. Utilice Tipo de recurso para centrarse únicamente en los buckets de S3. O bien, utilice ARN del recurso para dirigirse a un bucket de S3 específico.

Puede crear filtros adicionales mediante uno o varios de los siguientes criterios.

Nombre del criterio	Descripción	Cuándo utilizar este criterio
ID de cuenta	Desglosar por Cuenta de AWS.	Utilice este criterio para buscar evidencias relacionadas con una Cuenta de AWS específica.
Control	Desglosar por nombre de control.	Utilice este criterio para buscar evidencias relacionadas con un control específico.
Dominio de control	Desglosar por dominio de control.	Utilice este criterio para centrarse en un área temática específica mientras se prepara para una auditoría. Puede filtrar por dominio de control si está consultando una evaluación creada a partir de un marco estándar.

Nombre del criterio	Descripción	Cuándo utilizar este criterio
		Algunos ejemplos de dominios de control son la administr ación de identidades y accesos, el registro y la supervisión y la administración de redes.
Data source type (Tipo de origen de datos)	Desglosar por tipo de origen de datos.	Utilice este criterio para centrarse en un origen de datos específico. Establezca el valor en `Manual` para buscar evidencias que haya subido manualmente. De lo contrario, puede filtrar las evidencias automatizadas en función de su procedenc ia (por ejemplo `AWS Config`, `CloudTrail` , `Security Hub` o `AWS API calls`).
Nombre de evento	Desglosar por nombre de evento.	Utilice este criterio para centrarse en un evento específico con el que esté relacionada la evidencia. Un evento es el registro de una actividad en Cuenta de AWS. Por ejemplo, puede buscar el nombre de una llamada a la API, como la operación de IAM `AttachRolePolicy` que se usa para configurar los permisos. O bien, puede buscar una palabra clave de CloudTrail, como el evento `ConsoleLogin` que CloudTrail registra cuando un usuario inicia sesión en su cuenta.
ARN de recurso	Desglosar por nombre de recurso de Amazon (ARN).	Utilice este criterio para buscar evidencias relacionadas con un recurso específico de AWS.
Tipo de recurso	Desglosar por tipo de recurso.	Utilice este criterio para centrarse en el tipo de recurso que se está evaluando, como una instancia de Amazon EC2 o un bucket de S3.
Servicio	Desglosar por nombre de Servicio de AWS.	Utilice este criterio para buscar evidencias relacionadas con un Servicio de AWS específico, como Amazon EC2, Amazon S3 o AWS Config.

Nombre del criterio	Descripción	Cuándo utilizar este criterio
Categorías de servicio	Desglosar por categoría de Servicio de AWS.	Utilice este criterio para centrarse en una categoría específica de Servicio de AWS. Algunos ejemplos son seguridad, identidad y conformidad, base de datos y almacenamiento.

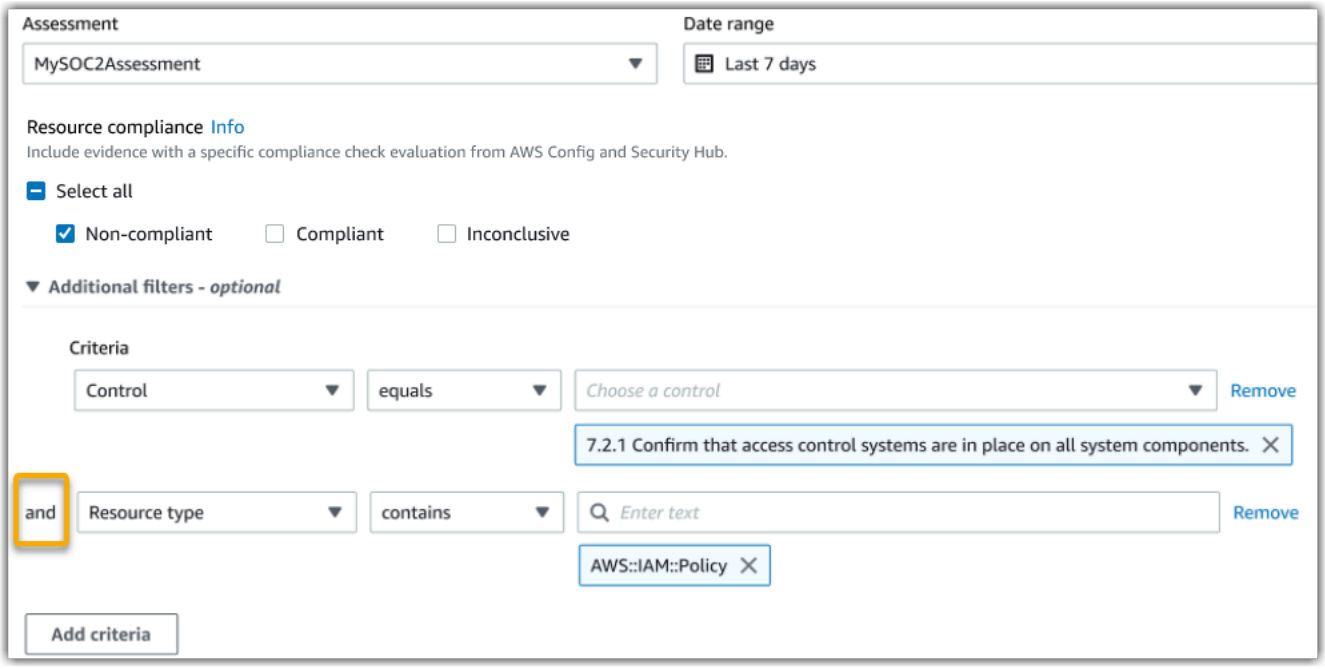
Combinar filtros

Comportamiento de criterios

Cuando especifica más de un criterio, Audit Manager aplica el operador `AND` a sus selecciones. Esto significa que todos los criterios se agrupan en una sola consulta y los resultados deben coincidir con todos los criterios combinados.

Ejemplo

En la siguiente configuración de filtros, el buscador de evidencias devuelve los recursos de no conformidad de los últimos 7 días para la evaluación denominada **`MySOC2Assessment`**. Además, los resultados se refieren tanto a una política de IAM como al control especificado.

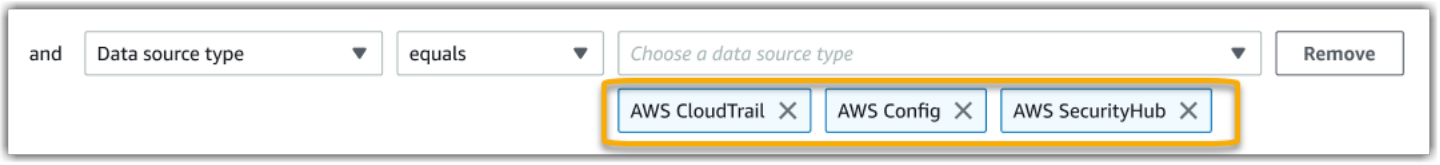


Comportamiento del valor de criterios

Cuando se especifica más de un valor de criterio, los valores se vinculan con un operador `OR`. El buscador de evidencias devuelve resultados que coinciden con cualquiera de estos valores de criterio.

Ejemplo

En la siguiente configuración de filtro, el buscador de evidencias devuelve los resultados de búsqueda que provienen de AWS CloudTrail, AWS Config o AWS Security Hub.



Agrupación de referencia

Puede agrupar los resultados de la búsqueda para una navegación más rápida. La agrupación le muestra la amplitud de los resultados de búsqueda y cómo están distribuidos en una dimensión específica.

Puede utilizar cualquiera de los siguientes grupos por valores.

Group by (Agrupar por)	Descripción
ID de cuenta	Agrupar los resultados por Cuenta de AWS.
Control	Agrupe los resultados por nombre de control.
Dominio de control	Agrupe los resultados por dominio de control.
Data source type (Tipo de origen de datos)	Agrupe los resultados por el tipo de origen de datos del que provienen las evidencias.
Nombre de evento	Agrupe los resultados por el nombre de un evento.
ARN de recurso	Agrupe resultados por nombre de recurso de Amazon (ARN).
Tipo de recurso	Agrupe los resultados por tipo de recurso.
Servicio	Agrupe los resultados por nombre de Servicio de AWS.

Group by (Agrupar por)	Descripción
Categorías de servicio	Agrupe los resultados por categoría de Servicio de AWS.

Ejemplos de casos de uso de

El buscador de evidencias puede ayudarle con varios casos de uso. En esta página se proporcionan algunos ejemplos y se sugieren los filtros de búsqueda que puede utilizar en cada situación.

Temas

Caso de uso 1: busque evidencias de no conformidad y organice las delegaciones

Este caso de uso es ideal si es responsable de conformidad, de protección de datos o un profesional de GRC encargado de supervisar la preparación de las auditorías.

Al supervisar la postura de conformidad de su organización, puede confiar en los equipos de socios para que le ayuden a solucionar los problemas. Puede utilizar el buscador de evidencias para ayudarle a organizar el trabajo para los equipos de sus socios.

Al aplicar filtros, puede centrarse en las evidencias de un área en concreto. Además, también puede estar en consonancia con las responsabilidades y el ámbito de cada equipo asociado con el que trabaje. Al realizar una búsqueda específica de este modo, puede utilizar los resultados de la búsqueda para identificar qué es exactamente lo que hay que corregir en cada área temática. A continuación, puede delegar las evidencias de no conformidad en el equipo asociado correspondiente para que las corrija.

Para este flujo de trabajo, siga los pasos para buscar evidencias. Utilice los siguientes filtros para buscar evidencias de no conformidad.

```
Assessment | <assessment name>
Date range | <date range>
```

```
Resource compliance | Non-compliant
```

A continuación, aplique filtros adicionales para el área en la que se está centrando. Por ejemplo, utilice el filtro Categoría de servicio para buscar recursos de no conformidad relacionados con la IAM. A continuación, comparta esos resultados con el equipo propietario de los recursos de la IAM para su organización. O bien, si está consultando una evaluación que se creó a partir de un marco estándar, puede usar el filtro de Dominio de control para encontrar evidencias de no conformidad relacionadas con el dominio de administración de identidades y accesos.

```
Control domain | <domain that you're focusing on>
or
Service category | <Servicio de AWS category that you're focusing on>
```

Cuando encuentre las evidencias que necesite, siga los pasos para generar un informe de evaluación a partir de los resultados de la búsqueda. Puede compartir este informe con su equipo asociado, que lo puede utilizar como lista de comprobación de las correcciones.

Caso de uso 2: identificar evidencias de conformidad

Este caso de uso es ideal si trabaja en SecOps, TI/DevOps u otro rol que posea y corrija los activos en la nube.

Como parte de una auditoría, es posible que se le pida que solucione los problemas relacionados con los recursos de los que dispone. Después de realizar este trabajo, puede utilizar el buscador de evidencias para validar que sus recursos son de conformidad.

Para este flujo de trabajo, siga los pasos para buscar evidencias. Utilice los siguientes filtros para buscar evidencias de conformidad.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Compliant
```

A continuación, aplique filtros adicionales para mostrar solo las evidencias de las que sea responsable. En función del ámbito de su propiedad, haga que la búsqueda sea tan segmentada como necesite. Los siguientes ejemplos de filtros están ordenados del más amplio al más preciso. Seleccione las opciones adecuadas para usted y sustituya el *<placeholder text>* por sus propios valores.

```
Control domain | <a subject area that you're responsible for>
Service category | <a category of Servicios de AWS that you own>
Service | <a specific Servicio de AWS that you own>
Resource type | <a collection of resources that you own>
Resource ARN | <a specific resource that you own>
```

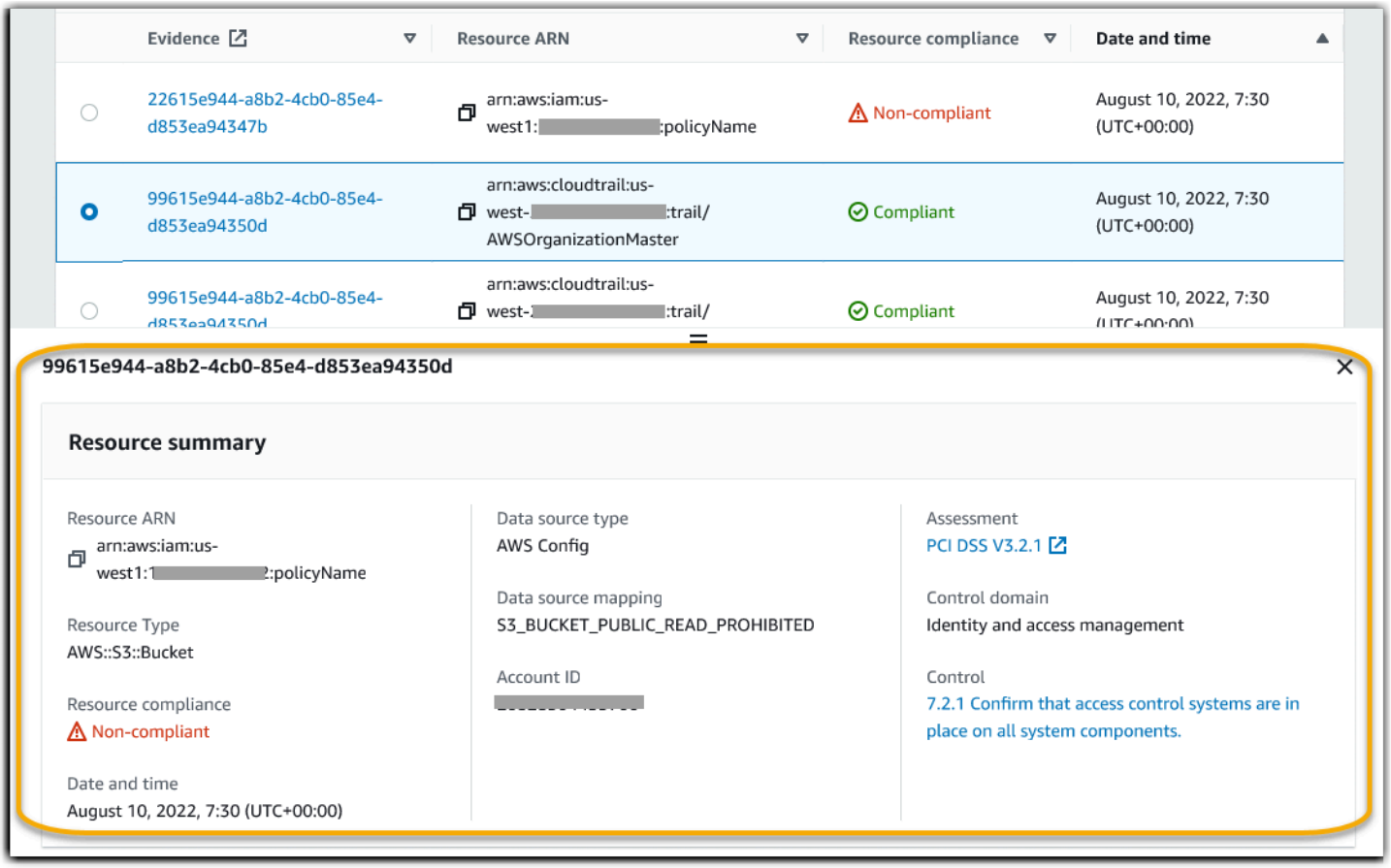
Si es responsable de varias instancias con el mismo criterio (por ejemplo, si es propietario de varios Servicios de AWS), puede agrupar los resultados por ese valor. Esto le proporcionará el total de coincidencias de evidencias para cada Servicio de AWS. A continuación, podrá obtener los resultados de los servicios de los que disponga.

Caso de uso 3: realizar una vista previa rápida de los recursos de evidencias

Este caso de uso es ideal para todos los clientes de Audit Manager.

Hasta ahora, revisar los datos de las evidencias individuales llevaba mucho tiempo. Si quería obtener una vista previa de las evidencias, tenía que ir directamente a esa evaluación y, a continuación, navegar por carpetas de evidencias muy jerarquizadas. Ahora, el buscador de evidencias ofrece una forma cómoda de obtener una vista previa de esta información. Para cada elemento de evidencia que coincida con su consulta de búsqueda, puede obtener una vista previa de los recursos individuales para dicha evidencia.

Para empezar, siga los pasos para buscar evidencias. A continuación, seleccione el botón de opción situado junto al resultado para ver un resumen de recursos en la página actual. Puede obtener una vista previa de cada recurso individual relacionado con un elemento de evidencia. Para ver todos los detalles de la evidencia de cualquier recurso, seleccione el nombre de la evidencia. Para obtener más información, consulte Vista previa de resúmenes de recursos.


Evidence
Resource ARN
Resource compliance
Date and time
22615e944-a8b2-4cb0-85e4-d853ea94347b
arn:aws:iam:us-west1:[redacted]:policyName
Non-compliant
August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d
arn:aws:cloudtrail:us-west-[redacted]:trail/AWSOrganizationMaster
Compliant
August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d
arn:aws:cloudtrail:us-west-[redacted]:trail/
Compliant
August 10, 2022, 7:30
99615e944-a8b2-4cb0-85e4-d853ea94350d
Resource summary
Resource ARN
arn:aws:iam:us-west1:[redacted]:policyName
Resource Type
AWS::S3::Bucket
Resource compliance
Non-compliant
Date and time
August 10, 2022, 7:30 (UTC+00:00)
Data source type
AWS Config
Data source mapping
S3_BUCKET_PUBLIC_READ_PROHIBITED
Account ID
[redacted]
Assessment
PCI DSS V3.2.1
Control domain
Identity and access management
Control
7.2.1 Confirm that access control systems are in place on all system components.

Centro de descargas de Audit Manager

El centro de descargas es el lugar donde puede encontrar y administrar todos los archivos descargables de Audit Manager. Al generar un informe de evaluación o exportar los resultados de una búsqueda desde el buscador de evidencias, los archivos aparecen en el centro de descargas.

Temas

Navegar por el centro de descargas

Para visitar el centro de descargas, abra la consola de Audit Manager en https://console.aws.amazon.com/auditmanager/home y, a continuación, elija Centro de descargas en el panel de navegación izquierdo.

Puede cambiar entre las siguientes pestañas para buscar los archivos por categoría.

Pestaña de informes de evaluación

En esta pestaña se muestran todos los informes de evaluación que ha generado. Los informes de evaluación permanecen disponibles en el centro de descargas hasta que los elimine.

Para ver el estado más reciente de su informe de evaluación, pulse el icono de actualización (#) para volver a cargar la tabla. En cada fila de la tabla de informes de evaluación se muestra el nombre del informe, su fecha de creación y uno de los siguientes estados:

- En curso: Audit Manager está generando el informe de evaluación.
- Listo: el informe de evaluación está disponible para su descarga.
- Error: no se pudo generar el informe de evaluación. En este caso, Audit Manager muestra un mensaje que describe el error. Para obtener más información sobre cómo resolver estos errores, consulte Informes de evaluación de solución de problemas.

Pestaña Exportaciones

Esta pestaña muestra todos los resultados de búsqueda del buscador de evidencias que ha exportado en los últimos siete días. Los archivos CSV se eliminan del centro de descargas

transcurridos siete días, pero permanecen disponibles en su bucket de S3 de destino de exportación. Para obtener instrucciones sobre cómo encontrar una exportación CSV del buscador de evidencias en su bucket de destino de S3, consulte Ver los resultados después de exportarlos.

Para ver el estado más reciente de sus exportaciones CSV, elija el icono de actualización (#) para recargar la tabla. Cada fila de la tabla de exportaciones muestra el nombre del archivo, su fecha de exportación y uno de los siguientes estados:

- En curso: Audit Manager está preparando el archivo CSV.
- Listo: la exportación se realizó correctamente y el archivo está disponible para su descarga.
- Error: se produjo un error en la exportación. En este caso, Audit Manager muestra un mensaje que describe el error. Para obtener información sobre cómo resolver estos errores, consulte Solución de problemas de exportación a CSV del buscador de evidencias.

> **Note**
>
> Tenga en cuenta que la pestaña de exportaciones también puede mostrar archivos CSV para consultas que haya realizado directamente en AWS CloudTrail Lake. Esto incluye las consultas realizadas en la consola de CloudTrail o mediante la API de CloudTrail. Las exportaciones de CloudTrail aparecerán en esta pestaña si consultó el almacén de datos de eventos de Audit Manager y eligió guardar los resultados en Amazon S3.

Descarga de un archivo

Siga estos pasos para descargar un archivo del centro de descargas.

Para descargar un archivo

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, seleccione Centro de descargas.
3. Seleccione la pestaña Informes de evaluación o la pestaña Exportaciones.
4. Seleccione el archivo que desea descargar y, a continuación, elija Descargar.

Para obtener instrucciones sobre cómo descargar un archivo del bucket de destino de S3, consulte Descargar un objeto en la Guía del usuario de Amazon Simple Storage Service (Amazon S3).

Eliminación de un archivo

Siga estos pasos para eliminar cualquier informe de evaluación que ya no necesite en el centro de descargas.

> **Note**
>
> Actualmente, no se permite eliminar exportaciones a archivos CSV desde el centro de descargas. Las exportaciones a CSV se eliminan automáticamente del centro de descargas transcurridos siete días.

Para eliminar un informe de evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, seleccione Centro de descargas.
3. Seleccione la pestaña Informes de evaluación.
4. Seleccione el informe de evaluación que desee eliminar y seleccione Eliminar.

Si desea eliminar un informe de evaluación o una exportación a CSV de su bucket de destino de S3, le recomendamos que complete esta tarea directamente en Amazon S3. Para obtener instrucciones, consulte Eliminación de objetos de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service (Amazon S3).

Biblioteca de marcos

Puede acceder a los marcos y gestionarlos desde la biblioteca de marcos en AWS Audit Manager.

Un marco de trabajo determina qué controles se prueban en un entorno durante un período de tiempo. Define los controles y sus asignaciones de origen de datos para un estándar o reglamento de cumplimiento determinado. También se utiliza para estructurar y automatizar las evaluaciones de Audit Manager. Puede utilizar los marcos como punto de partida para auditar su uso de Servicio de AWS y empezar a automatizar la recopilación de pruebas.

La biblioteca de marcos contiene un catálogo de marcos estándar y personalizados.

- Los Marcos estándar son marcos prediseñados que proporciona AWS. Estos marcos se basan en las prácticas recomendadas de AWS para diferentes estándares y reglamentos de cumplimiento. Estos incluyen el RGPD y la HIPAA. Los marcos estándar incluyen controles que se organizan en conjuntos de controles que se basan en el estándar o reglamento de cumplimiento que respalda el marco.

  Puede ver el contenido de los marcos estándar, pero no puede editarlos ni eliminarlos. Sin embargo, puede personalizar cualquier marco estándar para crear uno nuevo que se ajuste a sus requisitos específicos.
- Los Marcos personalizados son marcos personalizados de su propiedad. Puede crear un marco personalizado desde cero o personalizar un marco existente. Puede utilizar marcos personalizados para organizar los controles en conjuntos de controles de forma que se ajusten a sus requisitos específicos. Para obtener más información acerca de cómo administrar los controles, consulte Biblioteca de control.

Puede crear una evaluación a partir de un marco estándar o personalizado. Para obtener información sobre cómo crear y administrar las evaluaciones, consulte Evaluaciones en AWS Audit Manager.

> **Note**
>
> AWS Audit Manager ayuda a recopilar evidencias relevantes para verificar el cumplimiento de estándares y reglamentos de cumplimiento específicos. Sin embargo, no evalúa el cumplimiento en sí mismo. Por lo tanto, es posible que las pruebas recopiladas mediante AWS Audit Manager no incluyan toda la información sobre su uso de AWS que se necesita

para las auditorías. AWS Audit Manager no sustituye a los asesores legales ni a los expertos en cumplimiento.

En esta sección, se describe cómo puede crear y gestionar marcos personalizados en Audit Manager.

Temas

Acceder a los marcos disponibles en AWS Audit Manager

Puede ver todos los marcos disponibles en la página de la Biblioteca de marcos de la consola Audit Manager. Desde aquí, también puede crear una evaluación a partir de un marco, crear un marco personalizado o personalizar un marco existente.

También puede ver todos los marcos disponibles mediante la API de Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

Para visualizar los marcos disponibles utilice la consola

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija Biblioteca de marcos.
3. Elija la pestaña Marcos estándar o la pestaña Marcos personalizados para ver los marcos estándar y personalizados disponibles.
4. Elija cualquier nombre de marco para ver los detalles de ese marco.

AWS CLI

Para ver los marcos disponibles (AWS CLI)

Para ver los marcos en Audit Manager, utilice el comando list-assessment-frameworks y especifique un `--framework-type`. También puede recuperar una lista de marcos estándar. O puede recuperar una lista de marcos personalizados.

```
aws auditmanager list-assessment-frameworks --framework-type Standard
```

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Audit Manager API

Para ver los marcos disponibles (API)

Utilice la operación ListAssessmentFrameworks y especifique un frameworkType. O bien, puede devolver una lista de marcos estándar. O bien, puede devolver una lista de marcos personalizados.

Para obtener más información, elija uno de los enlaces anteriores para obtener más información en la referencia de la API de AWS Audit Manager. Esto incluye información sobre cómo utilizar la operación de `ListAssessmentFrameworks` y los parámetros en uno de los SDK de AWS específicos del lenguaje.

Ver los detalles de un marco

Puede revisar los detalles de un marco mediante la consola Audit Manager, la API Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

Para ver los detalles del marco utilice la consola

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija Biblioteca de marcos para ver una lista de marcos disponibles.

3. Seleccione la pestaña Marcos estándar o la pestaña Marcos personalizados para explorar los marcos disponibles.
4. Seleccione el nombre del marco para abrirlo.

Al abrir un marco, aparece una página de Detalles del marco. Las secciones de esta página y su contenido se describen a continuación.

Sección de detalles del marco

En esta sección, se proporciona información general sobre el marco. Contiene la información siguiente:

- Nombre del marco: el nombre del marco.
- Tipo de cumplimiento: estándar o reglamento de cumplimiento que admite el marco.
- Descripción: una descripción del marco, si se ha proporcionado una.
- Tipo de marco: especifica si el marco es estándar o personalizado.
- Conjuntos de controles: el número de conjuntos de controles que están asociados al marco.
- Controles: el número total de controles en el marco.
- Fuentes de control: el número de origen de datos de control de los que Audit Manager recopila pruebas.
- Etiquetas: las etiquetas que están asociadas al marco.

Si está viendo un marco personalizado, también se muestran los siguientes detalles:

- Creado por: la cuenta que creó el marco personalizado.
- Fecha de creación: la fecha en la que se creó el marco personalizado.
- Última actualización: fecha en la que se editó este marco por última vez.

Pestaña de controles

Esta pestaña muestra los controles del marco, agrupados por conjunto de controles. Contiene la información siguiente:

- Controles agrupados por conjunto de controles: seleccione el icono de vista en árbol para ver los controles que pertenecen a cada conjunto de controles.
- Tipo: especifica si el control es un control estándar o personalizado.
- Origen de datos: especifica el origen de datos de la que Audit Manager recopila las pruebas para ese control.

Pestaña de etiquetas

Esta pestaña enumera las etiquetas que están asociadas con el marco. Contiene la información siguiente:

- Clave: la clave de la etiqueta (por ejemplo, un estándar, un reglamento o una categoría de cumplimiento).
- Valor: el valor de la etiqueta.

AWS CLI

Para ver los detalles del marco (AWS CLI)

1. Para identificar el marco que desea revisar, ejecute el comando list-assessment-frameworks y especifique un `--framework-type`. También puede recuperar una lista de marcos estándar. O puede recuperar una lista de marcos personalizados.

   En el siguiente ejemplo, sustituya el *`texto del marcador de posición`* por `Custom` o `Standard`.

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom/Standard
   ```

   La respuesta devuelve una lista de marcos. Busque el marco que desea revisar y tome nota de su ID y del nombre de recurso de Amazon (ARN).
2. Para obtener los detalles del marco, ejecute el comando get-assessment-framework y especifique el `--framework-id`.

   En el siguiente ejemplo, reemplace el *`texto del marcador de posición`* con su propia información.

   ```
   aws auditmanager get-assessment-framework --framework-id a1b2c3d4-5678-90ab-
   cdef-EXAMPLE11111
   ```

   Los detalles del marco se devuelven en formato JSON. Para comprender estos datos, consulte el resultado de get-assessment-framework en la referencia de comandos de AWS CLI.
3. Para ver las etiquetas de un marco, utilice el comando list-tags-for-resource y especifique las `--resource-arn` para el marco.

En el siguiente ejemplo, reemplace el *texto del marcador de posición* con su propia información:

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:assessmentFramework/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Para obtener más información acerca del etiquetado en Audit Manager, consulte Etiquetado de recursos de AWS Audit Manager.

Audit Manager API

Para ver los detalles del marco (API)

1. Para identificar el marco que desea revisar, utilice la operación ListAssessmentFrameworks y especifique un frameworkType. O bien, puede devolver una lista de marcos estándar. O bien, puede devolver una lista de marcos personalizados.

   En la respuesta, busque el marco que desea revisar y anote el ID de marco y el nombre de recurso de Amazon (ARN).
2. Para obtener los detalles del marco, utilice la operación GetAssessmentFramework. En la solicitud, especifique el frameworkId que obtuvo en el paso 1.

   Los detalles del marco se devuelven en formato JSON. Para comprender estos datos, consulte los elementos de respuesta de GetAssessmentFramework en la referencia de la API de AWS Audit Manager.
3. Para ver las etiquetas del marco, utilice la operación ListTagsForResource. En la solicitud, especifique el framework ResourceArn que obtuvo en el paso 1.

Para obtener más información acerca del etiquetado en Audit Manager, consulte Etiquetado de recursos de AWS Audit Manager.

Para más información sobre estas operaciones de la API, consulte cualquiera de los enlaces anteriores en la referencia de la API de AWS Audit Manager. Esto incluye información sobre el uso de estas operaciones y parámetros en un lenguaje específico de un SDK de AWS.

Crear un marco personalizado

Puede acceder a los marcos y gestionarlos desde la biblioteca de marcos en AWS Audit Manager. Puede crear marcos personalizados para organizar los controles en conjuntos de controles de forma que se ajusten a sus requisitos específicos.

Existe dos maneras de crear un marco personalizado. Puede personalizar un marco existente o puede crear uno nuevo desde cero.

Temas

Crear un nuevo marco personalizado desde cero

Puede utilizar marcos personalizados en AWS Audit Manager para organizar los controles en conjuntos de controles de forma que se ajusten a sus requisitos específicos. Puede crear un nuevo marco personalizado desde cero en la biblioteca de marcos siguiendo estos pasos.

Temas

Paso 1: especificar los detalles del marco

Comience por especificar los controles que desea incluir en su marco personalizado.

Para especificar los detalles del marco

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija Biblioteca de marcos y, a continuación, Crear marco personalizado.

3. En Detalle del marco, introduzca un nombre, un estándar o reglamento de cumplimiento (opcional) y una descripción del marco (también opcional). Introduzca una palabra clave de estándar o reglamento de cumplimiento, como PCI_DSS o RGPD, para que pueda usar esta palabra clave para buscar su marco.
4. En Etiquetas, seleccione Añadir nueva etiqueta para asociar una etiqueta a su marco. Puede especificar una clave y un valor para cada etiqueta. La clave de la etiqueta es obligatoria. Puede utilizarla como criterio de búsqueda al buscar este marco en la biblioteca de marcos. Para obtener más información sobre las etiquetas de AWS Audit Manager, consulte Etiquetado de recursos de AWS Audit Manager.
5. Elija Siguiente.

Paso 2: especificar los controles de los conjuntos de controles

A continuación, especifique qué controles desea añadir a su marco y cómo desea organizarlos. Comience por agregar conjuntos de controles al marco y, a continuación, agregue controles al conjunto de controles.

> **Note**
>
> Al utilizar la consola de AWS Audit Manager para crear un marco personalizado, puede añadir hasta 10 conjuntos de controles para cada marco.
> Cuando utiliza la API de Audit Manager para crear un marco personalizado, puede crear más de 10 conjuntos de controles. Para añadir más conjuntos de controles de los que permite actualmente la consola, utilice la API CreateAssessmentFramework que proporciona Audit Manager.

Para especificar los controles de los conjuntos de controles

1. En Nombre del conjunto de controles, escriba un nombre para el conjunto de controles.
2. En Añadir un nuevo control al conjunto de controles, seleccione el tipo de control, y utilice la lista desplegable para seleccionar uno de los dos tipos de control: Controles estándar o Controles personalizados. Audit Manager proporciona los controles estándar, y los controles personalizados son los que usted crea.
3. Según la opción que haya seleccionado en el paso anterior, se muestra una lista de controles estándar o controles personalizados. Puede examinar la lista o realizar una búsqueda

introduciendo el nombre, el cumplimiento o la etiqueta del control. Seleccione uno o más controles y elija Añadir al conjunto de controles para añadirlos al conjunto de controles.

4. En la ventana emergente que aparece, seleccione Añadir al conjunto de controles para confirmar la adición.
5. En Revisar los controles seleccionados del conjunto de controles, revise los controles que aparecen en la lista de Controles seleccionados. Para agregar más controles a un conjunto de controles, repita los pasos 2 a 4. Para eliminar los controles no deseados del conjunto de controles, seleccione uno o más controles y elija Eliminar control.
6. Para añadir un nuevo conjunto de controles al marco, seleccione Añadir conjunto de controles en la parte inferior de la página. Puede eliminar conjuntos de controles no deseados seleccionando Eliminar conjunto de controles.
7. Cuando termine de añadir conjuntos de controles y controles, elija Siguiente.

Paso 3: revisar y crear el marco

Revise la información de su marco. Para modificar la información de un paso, seleccione Editar.

Cuando haya terminado, elija Crear un marco personalizado.

¿Qué puedo hacer ahora?

Después de crear el nuevo marco personalizado, puede crear una evaluación a partir del marco. Para obtener más información, consulte Creación de las evaluaciones.

También puede crear un marco personalizado utilizando un marco existente. Para obtener más información, consulte Personalizar un marco existente.

Para obtener instrucciones sobre cómo editar el marco personalizado, consulte Editar un marco personalizado.

Personalizar un marco existente

Con los marcos personalizados en AWS Audit Manager, puede organizar los controles en conjuntos de controles de forma que se ajusten a sus requisitos específicos. En lugar de crear un marco personalizado desde cero, puede utilizar un marco existente como punto de partida y personalizarlo. Al hacerlo, el marco existente permanece en la biblioteca de marcos y se crea un nuevo marco personalizado con sus ajustes personalizados.

Puede seleccionar cualquier marco existente para personalizarlo. Puede ser un marco estándar o un marco personalizado.

En la biblioteca de marcos, en la lista desplegable Crear un marco personalizado, elija Personalizar marco existente. Siga estos pasos para personalizar el marco.

Temas

Paso 1: especificar los detalles del marco

Todos los detalles del marco, excepto las etiquetas, se transfieren del marco original. Revise y modifique estos detalles según sea necesario.

Para especificar los detalles del marco

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija Biblioteca de marcos.
3. Elija el marco que desee personalizar y, en la lista desplegable Crear marco personalizado, elija Personalizar marco existente.
4. En la ventana emergente que aparece, introduzca un nombre para el nuevo marco personalizado y seleccione Personalizar.
5. En Detalles del marco, revise el nombre, el tipo de cumplimiento y la descripción del marco y modifíquelos según sea necesario. El tipo de cumplimiento debe indicar el estándar de cumplimiento o la normativa asociada a su marco. Puede utilizar esta palabra clave para buscar su marco.
6. En Etiquetas, seleccione Añadir nueva etiqueta para asociar una etiqueta a su marco. Puede especificar una clave y un valor para cada etiqueta. La clave de la etiqueta es obligatoria y se puede utilizar como criterio de búsqueda al buscar este marco en la biblioteca de marcos. Para obtener más información sobre las etiquetas de AWS Audit Manager, consulte Etiquetado de recursos de AWS Audit Manager.
7. Elija Siguiente.

Paso 2: especifique los controles para añadirlos a los conjuntos de controles

Los conjuntos de controles se transfieren del marco original. Personalice la configuración actual añadiendo más controles o quitando los controles existentes según sea necesario.

> **Note**
>
> Cuando utiliza la consola de AWS Audit Manager para personalizar un marco, puede añadir hasta 10 conjuntos de controles para cada marco.
> Cuando utiliza la API de Audit Manager para crear un marco personalizado, puede añadir más de 10 conjuntos de controles. Para añadir más conjuntos de controles de los que permite actualmente la consola, utilice la API CreateAssessmentFramework que proporciona Audit Manager.

Para especificar los controles del conjunto de controles

1. En Nombre del conjunto de controles, personalice el nombre del conjunto de controles según sea necesario.
2. En Añadir un nuevo control al conjunto de controles, añada un nuevo control mediante la lista desplegable para seleccionar uno de los dos tipos de control: Controles estándar o Controles personalizados.
3. Según la opción que haya seleccionado en el paso anterior, se muestra una lista de controles estándar o controles personalizados. Puede examinar esta lista o realizar una búsqueda introduciendo el nombre del control, el cumplimiento o las etiquetas para localizar los controles que desee añadir. Seleccione uno o más controles y elija Añadir al conjunto de controles para añadirlos a este conjunto de controles.
4. En la ventana emergente que aparece, seleccione Añadir al conjunto de controles para confirmar la adición.
5. En Revisar los controles seleccionados del conjunto de controles, revise los controles que aparecen en la lista de Controles seleccionados. Para agregar más controles a un conjunto de controles, repita los pasos 2 a 4. Para eliminar los controles no deseados del conjunto de controles, seleccione uno o más controles y elija Eliminar control.
6. Para añadir un nuevo conjunto de controles al marco, seleccione Añadir conjunto de controles en la parte inferior de la página. Puede eliminar conjuntos de controles no deseados seleccionando Eliminar conjunto de controles.

7. Cuando termine de añadir conjuntos de controles y controles, elija Siguiente.

Paso 3: revisar y crear el marco

Revise la información de su marco. Para modificar la información de un paso, seleccione Editar.

Cuando haya terminado, elija Crear un marco personalizado.

¿Qué puedo hacer ahora?

Después de crear el nuevo marco personalizado, puede crear una evaluación a partir del marco. Para obtener más información, consulte Creación de las evaluaciones.

Para obtener instrucciones sobre cómo editar el marco personalizado, consulte Editar un marco personalizado.

Editar un marco personalizado

Puede utilizar marcos personalizados en AWS Audit Manager para organizar los controles en conjuntos de controles que se ajusten a sus necesidades específicas. Puede usar la biblioteca de marcos para buscar y editar un marco personalizado siguiendo estos pasos.

Temas

Paso 1: editar los detalles del marco

Comience por revisar y editar los detalles del marco existente.

Para editar los detalles del marco

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija la Biblioteca de marcos y, a continuación, elija la pestaña Marcos personalizados.
3. Seleccione el marco que desee editar, elija Acciones y, a continuación, elija Editar.

- Como alternativa, puede abrir un marco personalizado y elegir Actciones y Editar en la parte superior derecha de la página de resumen de la evaluación.

4. En Detalles del marco, revise el nombre, el tipo de cumplimiento y la descripción del marco y realice los cambios necesarios.
5. Elija Siguiente.

> **Tip**
>
> Para editar las etiquetas de un marco, abra el marco y elija la pestaña de etiquetas del marco. Allí puede ver y editar las etiquetas asociadas al marco.

Paso 2: editar los controles del conjunto de controles

A continuación, revise y edite los controles y conjuntos de controles del marco.

> **Note**
>
> Al utilizar la consola de AWS Audit Manager para editar un marco personalizado, puede añadir hasta 10 conjuntos de controles para cada marco.
> Cuando utiliza la API de Audit Manager para editar un marco personalizado, puede añadir más de 10 conjuntos de controles. Para añadir más conjuntos de controles de los que permite actualmente la consola, utilice la API UpdateAssessmentFramework que proporciona Audit Manager.

Para editar los controles

1. En Nombre del conjunto de controles , revise y edite el nombre del conjunto de controles según sea necesario.
2. En Añadir un control nuevo al conjunto de controles, puede añadir un control. Utilice la lista desplegable para seleccionar uno de los dos tipos de control: Controles estándar o Controles personalizados.
3. En función de la opción que haya seleccionado en el paso anterior, se mostrará una lista de controles estándar o controles personalizados. Puede buscar conjuntos de controles en la lista. O bien, puede buscar introduciendo el nombre del control, el origen de datos o las etiquetas

para localizar los controles que desee agregar. Seleccione uno o más controles y elija Añadir al conjunto de controles para añadirlos a este conjunto de controles.

4. En la ventana emergente que aparece, seleccione Añadir al conjunto de controles para confirmar la adición.
5. En Revisar los controles seleccionados del conjunto de controles, revise y edite los controles que aparecen actualmente en la lista de Controles seleccionados. Para agregar más controles a un conjunto de controles, repita los pasos 2 a 4. Elimine los controles no deseados del conjunto de controles seleccionando uno o más controles y eligiendo Eliminar control.
6. Para añadir un nuevo conjunto de controles al marco, seleccione Añadir conjunto de controles en la parte inferior de la página. Elimine los conjuntos de controles no deseados seleccionando Eliminar conjunto de controles .
7. Cuando termine de añadir conjuntos de controles y controles, elija Siguiente.

Paso 3. Revise y actualice el marco

Revise la información de su marco. Para modificar la información de un paso, seleccione Editar.

Cuando haya finalizado, elija Save changes (Guardar cambios).

Eliminar un marco personalizado

Puede utilizar la biblioteca de marcos para buscar y eliminar un marco personalizado no deseado. También puede eliminar marcos personalizados mediante la API Audit Manager o AWS Command Line Interface (AWS CLI).

> **Note**
>
> La eliminación de un marco personalizado no afecta a ninguna evaluación existente que se haya creado a partir del marco antes de su eliminación.

Audit Manager console

Para eliminar un marco personalizado utilice la consola

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.

2. En el panel de navegación izquierdo, elija la Biblioteca de marcos y, a continuación, elija la pestaña Marcos personalizados.
3. Seleccione el marco que desee eliminar, elija Acciones y, a continuación, elija Eliminar.
   - Como alternativa, puede abrir un marco personalizado y elegir Acciones y Eliminar en la parte superior derecha de la página de resumen del marco.
4. En la ventana emergente, seleccione Eliminar para confirmar la eliminación.

AWS CLI

Para eliminar un marco personalizado (AWS CLI)

1. En primer lugar, identificar el marco personalizado que desea eliminar. Para ello, ejecute el comando list-assessment-frameworks y especifique el `--framework-type` como `Custom`.

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom
   ```

   La respuesta devuelve una lista de marcos personalizados. Busque el marco personalizado que desea eliminar y tome nota del ID del marco.
2. A continuación, ejecute el comando delete-assessment-framework y especifique el `--framework-id` del marco que desea eliminar.

   En el siguiente ejemplo, reemplace el *`texto del marcador de posición`* con su propia información.

   ```
   aws auditmanager delete-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

Para eliminar un marco personalizado (API)

1. Utilice la operación ListAssessmentFrameworks y especifique el frameworkType como `Custom`. En la respuesta, busque el marco personalizado que desea eliminar y anote el ID del marco.
2. Utilice la operación DeleteAssessmentFramework para eliminar el marco. En la solicitud, utilice el parámetro frameworkId para especificar el marco que desea eliminar.

Para más información sobre estas operaciones de la API, consulte cualquiera de los enlaces anteriores en la referencia de la API de AWS Audit Manager. Esto incluye información sobre el uso de estas operaciones y parámetros en un lenguaje específico de un SDK de AWS.

Compartir un marco personalizado

Puede utilizar la característica de compartir marcos de AWS Audit Manager para replicar rápidamente los marcos personalizados que cree. Puede compartir sus marcos personalizados con otro Cuenta de AWS o replicar sus marcos en otro Región de AWS bajo su propia cuenta. A continuación, el destinatario podrá acceder a su marco personalizado y utilizarlo para crear evaluaciones. Pueden hacerlo sin tener que repetir ninguno de sus esfuerzos de configuración para ese marco.

Para compartir un marco personalizado, debe crear una solicitud de uso compartido. El destinatario de la solicitud de uso compartido tiene entonces 120 días para aceptarla o rechazarla. Cuando aceptan la solicitud de uso compartido, Audit Manager replica el marco personalizado compartido en su biblioteca de marcos. Además de replicar el marco personalizado, Audit Manager también replica todos los conjuntos de controles personalizados y los controles personalizados que formen parte de ese marco. Estos controles personalizados se agregan luego a la biblioteca de controles del destinatario. Audit Manager no replica los marcos o controles estándar. De forma predeterminada, están disponibles en todas las Cuentas de AWS y regiones en las que Audit Manager esté activado.

La característica para compartir marcos solo está disponible en el nivel de pago. Sin embargo, no hay cargos adicionales por compartir un marco personalizado o por aceptar una solicitud de uso compartido. Para obtener más información acerca de los precios de AWS Audit Manager, visite la página de precios de AWS Audit Manager.

> **Important**
>
> No puede compartir un marco personalizado derivado de un marco estándar si el marco estándar ha sido designado como no apto para ser compartido por AWS, a menos que haya obtenido el permiso del propietario del marco estándar para hacerlo. Para ver qué marcos estándar no se pueden compartir y obtener más información, consulte Elegibilidad para compartir marcos.

En las siguientes secciones de esta guía, se describen los aspectos importantes que debe saber sobre el uso compartido de marcos. También proporcionan instrucciones sobre cómo puede compartir sus marcos personalizados y responder a las solicitudes de uso compartido.

Temas

> **Tip**
>
> Si no está familiarizado con los marcos personalizados de Audit Manager y cómo crearlos, puede obtener más información en la página Creación de un marco personalizado de esta guía.

Conceptos y terminología del uso compartido de marcos

Si conoce los siguientes conceptos clave, puede sacar más provecho de la característica de uso compartido de marcos personalizados AWS Audit Manager.

Sender

Este es el creador de una solicitud de uso compartido y el Cuenta de AWS donde existe el marco personalizado. Los remitentes pueden compartir marcos personalizados con cualquier Cuenta de AWS. O bien, replican un marco personalizado en cualquier Región de AWS compatible bajo su propia cuenta.

Recipient

Es el consumidor del marco compartido. Los destinatarios pueden aceptar o rechazar una solicitud de uso compartido de un remitente.

> **Note**
>
> Un destinatario puede ser una cuenta de administrador delegado. Sin embargo, no puede compartir marcos personalizados con una cuenta de administración de AWS Organizations.

Elegibilidad del marco

Solo puede compartir marcos personalizados. De forma predeterminada, los marcos estándar ya están presentes en todos los Cuentas de AWS y Regiones de AWS en los que AWS Audit Manager está habilitado. Además, los marcos personalizados que comparta no deben contener datos confidenciales. Esto incluye los datos que se encuentran en el propio marco, sus conjuntos de controles y cualquiera de los controles personalizados que forman parte del marco personalizado.

> **Important**
>
> Algunos de los marcos estándar que ofrece AWS Audit Manager contienen material protegido por derechos de autor que está sujeto a acuerdos de licencia. Los marcos personalizados pueden contener contenido derivado de estos marcos. No puede compartir un marco personalizado derivado de un marco estándar si el marco estándar ha sido designado como no apto para ser compartido por AWS, a menos que haya obtenido el permiso del propietario del marco estándar para hacerlo.
> Para saber qué marcos estándar se pueden compartir, consulte la siguiente tabla.

Nombre del marco estándar	Versiones personalizadas aptas para compartir
Essential Eight del Centro Australiano de Ciberseguridad (Australian Cyber Security Centre, ACSC)	Sí
Manual de seguridad de la información del Centro Australiano de Ciberseguridad (ACSC)	Sí

Nombre del marco estándar	Versiones personalizadas aptas para compartir
Ejemplo de marco AWS Audit Manager	Sí
Medidas de seguridad de AWS Control Tower	Sí
Marco de prácticas recomendadas de IA generativa v1 de AWS	Sí
AWS License Manager	Sí
Prácticas recomendadas de seguridad básica de AWS	Sí
Prácticas operativas recomendadas de AWS	Sí
Marco de AWS Well-Architected	Sí
Centro Canadiense de Ciberseguridad - Medio	No

Nombre del marco estándar	Versiones personalizadas aptas para compartir
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0, nivel 1	 No
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0, nivel 1 y 2	 No
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0, nivel 1	 No
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0, nivel 1 y 2	 No
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0, nivel 1	 No
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0, nivel 1 y 2	 No
Controles CIS v7.1 IG1	 Sí
Controles CIS v8 IG1	 No

Nombre del marco estándar	Versiones personalizadas aptas para compartir
Referencia moderada de FedRAMP	 Sí
RGPD	 Sí
Ley Gramm-Leach-Bliley (GLBA)	 Sí
GxP 21 CFR Parte 11	 Sí
GxP UE Anexo 11	 Sí
Norma de seguridad de la HIPAA de 2003	 Sí
Norma general de seguridad definitiva de la HIPAA de 2013	 Sí
Anexo A de la norma de la ISO/IEC 27001:2013	 No

Nombre del marco estándar	Versiones personalizadas aptas para compartir
NIST 800-53 (Rev. 5) Low-Moderate-High	Sí
Marco de Ciberseguridad del NIST versión 1.1	Sí
NIST SP 800-171 Rev. 2	Sí
PCI DSS v3.2.1	No
PCI DSS v4.0	No
SOC 2	No

Solicitud de uso compartido

Para compartir un marco personalizado, debe crear una solicitud de uso compartido. La solicitud de uso compartido especifica un destinatario y le notifica que hay un marco personalizado disponible. Los destinatarios tienen 120 días para aceptar o rechazar una solicitud de uso compartido. Si no se realiza ninguna acción en 120 días, la solicitud de uso compartido vence y el destinatario pierde la posibilidad de añadir el marco personalizado a su biblioteca de marcos. Los remitentes y los destinatarios pueden ver las solicitudes de uso compartido y tomar medidas al respecto desde la página de solicitudes de uso compartido de la biblioteca de marcos.

Estado de la solicitud de uso compartido

Las solicitudes de uso compartido pueden tener cualquiera de los siguientes estados.

- Activa: indica una solicitud de uso compartido que se envió correctamente al destinatario y que está esperando su respuesta.
- Vencimiento: indica una solicitud de uso compartido que vence en los próximos 30 días.
- Compartida: indica una solicitud de uso compartido que el destinatario ha aceptado.
- Inactiva: indica que se trata de una solicitud de uso compartido que se revocó, rechazó o expiró antes de que el destinatario tomara medidas.
- En proceso de replicación: indica una solicitud de uso compartido aceptada que se está replicando en la biblioteca de marcos del destinatario.
- Error: indica que la solicitud de uso compartido no se envió correctamente al destinatario.

Notificaciones de solicitud de uso compartido

Audit Manager notifica a los destinatarios cuando reciben una solicitud de uso compartido. Tanto los destinatarios como los remitentes reciben una notificación cuando una solicitud de uso compartido vence dentro de los próximos 30 días.

- Para los destinatarios, aparece un punto de notificación azul junto a las solicitudes recibidas con el estado Activo o Vencido. El destinatario puede resolver la notificación aceptando o rechazando la solicitud de uso compartido.
- En el caso de los remitentes, aparece un punto de notificación azul junto a las solicitudes enviadas con el estado de Vencido. La notificación se resuelve cuando el destinatario acepta o rechaza la solicitud. De lo contrario, se resuelve cuando vence la solicitud. Además, el remitente puede resolver la notificación revocando la solicitud de uso compartido.

Titularidad del remitente

Los remitentes mantienen el acceso total a los marcos personalizados que comparten. Pueden cancelar las solicitudes de uso compartido activas en cualquier momento revocando la solicitud de uso compartido antes de que caduque. Sin embargo, una vez que el destinatario acepta una solicitud de uso compartido, el remitente ya no puede revocar el acceso del destinatario a ese marco personalizado. Esto se debe a que, cuando el destinatario acepta la solicitud, Audit Manager crea una copia independiente del marco personalizado en la biblioteca de marcos del destinatario.

Además de replicar el marco personalizado del remitente, Audit Manager también replica todos los conjuntos de controles personalizados y los controles personalizados que formen parte de ese marco. Sin embargo, Audit Manager no replica ninguna etiqueta adjunta al marco personalizado.

Titularidad del destinatario

Los destinatarios tienen acceso total a los marcos personalizados que aceptan. Cuando el destinatario acepta la solicitud, Audit Manager replica el marco personalizado en la pestaña marcos personalizados de su biblioteca de marcos. Los destinatarios pueden administrar el marco personalizado compartido de la misma manera que cualquier otro marco personalizado. Los destinatarios pueden compartir los marcos personalizados que reciben de otros remitentes. Los destinatarios no pueden impedir que los remitentes envíen solicitudes de uso compartido.

Vencimiento del marco compartido

Cuando un remitente crea una solicitud de uso compartido, Audit Manager establece que la solicitud caduque después de 120 días. Los destinatarios pueden aceptar el marco compartido y obtener acceso a él antes de que caduque la solicitud. Si un destinatario no acepta durante este tiempo, la solicitud de uso compartido caducará. Después de este punto, queda un registro de la solicitud de uso compartido caducada en su historial. Las instantáneas de los marcos compartidos caducados se archivan en un bucket de S3 con un TTL de un año para fines de auditoría.

Los remitentes pueden optar por revocar una solicitud de uso compartido en cualquier momento antes de que caduque.

Almacenamiento y respaldo de datos en un marco compartido

Cuando crea una solicitud de uso compartido, Audit Manager almacena una instantánea de su marco personalizado en el este de EE. UU. (Norte de Virginia)Región de AWS. Audit Manager también almacena una copia de seguridad de la misma instantánea en el oeste de EE. UU. (Oregón)Región de AWS.

Audit Manager elimina la instantánea y la instantánea de respaldo cuando ocurre uno de los siguientes eventos:

- El remitente revoca la solicitud de uso compartido.
- El destinatario rechaza la solicitud de uso compartido.
- El destinatario detecta un error y no acepta correctamente la solicitud de uso compartido.
- La solicitud de uso compartido caduca antes de que el destinatario responda a la solicitud.

Cuando un remitente vuelve a enviar una solicitud de uso compartido, la instantánea se sustituye por una versión actualizada que se corresponde con la última versión del marco personalizado.

Cuando un destinatario acepta una solicitud de uso compartido, la instantánea se replica en su Cuenta de AWS según el Región de AWS especificado en la solicitud de uso compartido.

Control de versiones de un marco compartido

Al compartir un marco personalizado, Audit Manager crea una copia independiente de ese marco en las Cuenta de AWS y región especificadas. Esto significa que debe tener en cuenta los siguientes puntos:

- El marco compartido que acepta el destinatario es una instantánea del marco en el momento de la creación de la solicitud de uso compartido. Si actualiza el marco personalizado original después de enviar una solicitud de uso compartido, la solicitud no se actualiza automáticamente. Para compartir la última versión del marco actualizado, puede volver a enviar la solicitud de uso compartido. La fecha de caducidad de esta nueva instantánea es de 120 días a partir de la fecha en que se volvió a compartir.
- Al compartir un marco personalizado con otro Cuenta de AWS y, a continuación, eliminarlo de la biblioteca de marcos, el marco personalizado compartido permanece en la biblioteca de marcos del destinatario.
- Cuando comparte un marco personalizado con otra Región de AWS de su cuenta y, a continuación, elimina ese marco personalizado en la primera Región de AWS, el marco personalizado permanece en la segunda región.
- Al eliminar un marco personalizado compartido después de aceptarlo, los controles personalizados que se hayan replicado como parte del marco personalizado permanecen en la biblioteca de controles.

Envío de una solicitud de uso compartido para un marco personalizado

Este tutorial describe cómo compartir sus marcos personalizados entre Cuentas de AWS y Regiones de AWS.

Cuando comparte un marco personalizado, Audit Manager crea una instantánea del marco y envía una solicitud de uso compartido al destinatario. El destinatario tiene 120 días para aceptar el marco compartido. Cuando lo aceptan, Audit Manager replica el marco personalizado compartido en su biblioteca de marcos en el Región de AWS especificado. Si desea replicar un marco personalizado en otra región con su propia cuenta, utilice el siguiente tutorial e introduzca su propia identificación de Cuenta de AWS como identificación de la cuenta del destinatario.

Este tutorial abarca los siguientes pasos:

1. Seleccione un marco para compartir: explore la biblioteca de marcos para encontrar el marco personalizado que desea compartir.
2. Enviar una solicitud de uso compartido: especifique un destinatario y envíele una solicitud de uso compartido del marco personalizado.
3. Ver las solicitudes enviadas: consulte su historial de solicitudes de uso compartido y compruebe el estado de las solicitudes enviadas.
4. (Opcional) Revocar la solicitud de uso compartido: revoque la solicitud de uso compartido antes de que caduque.

Requisitos previos

Antes de comenzar este tutorial, asegúrese de cumplir las siguientes condiciones:

- Está familiarizado con la terminología y los conceptos de uso compartido del marco de Audit Manager.
- El marco personalizado que desea compartir es apto para compartirse y existe en la biblioteca de marcos de su entorno de AWS Audit Manager.
- El destinatario ya habilitó AWS Audit Manager en el Región de AWS en el que desea compartir el marco personalizado.
- El destinatario no es una cuenta de administración de AWS Organizations.

> **Tip**
>
> Antes de empezar, anote la ID de Cuenta de AWS con la que desea compartir su marco personalizado. Puede ser la ID de su propia cuenta, si su objetivo es replicar el marco a otro Región de AWS de su cuenta. Necesita esta información para el paso 2 del tutorial.

> **Important**
>
> No comparta marcos personalizados que contengan datos confidenciales. Esto incluye los datos que se encuentran dentro del propio marco, sus conjuntos de controles y cualquiera de los controles personalizados que componen el marco personalizado. Para obtener más información, consulte el Elegibilidad del marco.

Paso 1: identifique el marco personalizado que desea compartir

Comience por identificar el marco personalizado que desea compartir. Puede encontrar una lista de todos los marcos personalizados disponibles en la página de la Biblioteca de marcos de Audit Manager.

Para ver los marcos personalizados disponibles

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Biblioteca de marcos.
3. Elija la pestaña Marcos personalizados. Esto muestra una lista de los marcos personalizados disponibles. Puede elegir cualquier nombre de marco para ver los detalles de ese marco personalizado.

Paso 2: Enviar una solicitud de uso compartido

A continuación, especifique un destinatario y envíele una solicitud de uso compartido del marco personalizado. El destinatario tiene 120 días para responder a la solicitud de uso compartido antes de que caduque.

Para enviar una solicitud de uso compartido

1. En la pestaña Marcos personalizados de la biblioteca de marcos, elija el nombre de un marco para abrir la página de detalles. Desde aquí, seleccione Acciones y, a continuación, seleccione Compartir marco personalizado.
   - También puede seleccionar un marco personalizado de la lista de la biblioteca de marcos, elegir Acciones y, a continuación, elegir Compartir marco personalizado. Según el tamaño del marco personalizado, este método puede tardar unos segundos mientras Audit Manager prepara la solicitud de uso compartido.
2. Revise el aviso que aparece en el cuadro de diálogo.
   - Si no está seguro de si puede compartir su marco personalizado, consulte la Elegibilidad del marco para obtener más información.
   - Si su marco tiene controles que utilizan normas de AWS Config personalizadas como origen de datos, le recomendamos que se ponga en contacto con el destinatario para informarle. A continuación, el destinatario podrá crear y habilitar las mismas normas de AWS Config en su

instancia de AWS Config. Para obtener más información, consulte Mi marco compartido tiene controles que utilizan reglas AWS Configpersonalizadas como origen de datos. ¿Puede el destinatario recopilar pruebas para estos controles?.

3. Introduzca **`agree`** y, a continuación, seleccione Aceptar para continuar.
4. En la siguiente pantalla, siga estos pasos:
   - En Cuenta de AWS, introduzca la ID de cuenta del destinatario. Puede ser su propia ID de cuenta.
   - En Región de AWS, seleccione la región del destinatario en la lista desplegable.
   - (Opcional) En Enviar mensaje al destinatario, introduzca un comentario opcional sobre el marco personalizado que va a compartir.
   - En Detalles del marco personalizado, revise los detalles para confirmar que desea compartir este marco.
5. Elija Compartir.

> **Note**
>
> Tenga en cuenta los siguientes puntos:
>
> - Al compartir un marco personalizado con otro Cuenta de AWS, el marco se replica solo en el Región de AWS especificado. Tras aceptar la solicitud de uso compartido, el destinatario podrá replicar el marco en todas las regiones según sea necesario.
> - Al compartir marcos personalizados en Regiones de AWS, procesar las acciones de solicitud de uso compartido puede tardar hasta 10 minutos. Tras enviar una solicitud de uso compartido entre regiones, le recomendamos que vuelva a consultarla más tarde para confirmar que la solicitud se ha enviado correctamente.
> - Al enviar una solicitud de uso compartido, Audit Manager toma una instantánea del marco personalizado en el momento de la creación de la solicitud de uso compartido. Si actualiza el marco personalizado después de enviar una solicitud de uso compartido, la solicitud no se actualiza automáticamente. Para compartir la última versión de un marco actualizado, puede volver a enviar la solicitud de uso compartido. La fecha de caducidad de esta nueva instantánea es de 120 días a partir de la fecha en que se volvió a compartir.

Paso 3: ver las solicitudes enviadas

Puede seleccionar la pestaña Solicitudes enviadas para ver una lista de todas las solicitudes de uso compartido que ha enviado. Puede filtrar esta lista según sea necesario. Por ejemplo, puede aplicar filtros para mostrar solo las solicitudes que caduquen en los próximos 30 días.

Para ver y filtrar las solicitudes enviadas

1. En el panel de navegación, elija Solicitudes de uso compartido.
2. Seleccione la pestaña Solicitudes enviadas.
3. (Opcional) Aplique filtros para ajustar qué solicitudes enviadas están visibles. Para ello, busque la lista desplegable Todos los estados y cambia el filtro por uno de los siguientes.

   - Activo: este filtro muestra las solicitudes de uso compartido que están pendientes de respuesta por parte del destinatario.
   - Compartido: este filtro muestra las solicitudes de uso compartido que fueron aceptadas por el destinatario. El marco personalizado compartido ahora existe en la biblioteca de marcos del destinatario.
   - Inactivo: este filtro muestra las solicitudes de uso compartido que se rechazaron, revocaron o vencieron antes de que el destinatario actuara. Elija la palabra Inactivo para ver más detalles.
   - Vencimiento: este filtro muestra las solicitudes de uso compartido que vencen en los próximos 30 días.
   - Error: este filtro muestra las solicitudes de uso compartido que no se enviaron correctamente al destinatario. Seleccione la palabra Falló para ver más detalles.

> **Note**
>
> El procesamiento de una solicitud de uso compartido puede tardar hasta 15 minutos en procesarse. En consecuencia, si se produce un error al enviar la solicitud de uso compartido al destinatario, es posible que el estado Falló no se muestre inmediatamente. Le recomendamos que vuelva a comprobarlo más tarde para confirmar que su solicitud de uso compartido se ha enviado correctamente.
> Para obtener información sobre cómo proceder si se produce un error, consulte Solución de problemas de solicitudes de uso compartido.

Paso 4 (opcional): revocar la solicitud de uso compartido

Si necesita cancelar una solicitud de uso compartido activa antes de que caduque, puede revocar la solicitud en cualquier momento. Este paso es opcional. Si no realiza ninguna acción, el destinatario pierde la capacidad de aceptar la solicitud de uso compartido después de la fecha de caducidad.

Para revocar una solicitud de uso compartido

1. En el panel de navegación, elija Solicitudes de uso compartido.
2. Seleccione la pestaña Solicitudes enviadas.
3. Seleccione el marco que desee revocar y elija Revocar solicitud.
4. En la ventana emergente que aparece, seleccione Revocar.

> **Note**
>
> Sólo puede revocar el acceso a las solicitudes de uso compartido que tengan un estado Activo o Vencido. Una vez que el destinatario acepte una solicitud de uso compartido, ya no podrá revocar su acceso a ese marco personalizado. Esto se debe a que ahora existe una copia del marco personalizado en la biblioteca de marcos del destinatario.
> Al compartir marcos entre Regiones de AWS, procesar las acciones de solicitud de uso compartido puede tardar hasta 10 minutos. Después de revocar una solicitud de uso compartido entre regiones, le recomendamos que vuelva a comprobarlo más tarde para confirmar que la solicitud de uso compartido se ha revocado correctamente.

Reenviar una solicitud de uso compartido para actualizar el marco

Puede enviar una solicitud de uso compartido para un marco personalizado y luego actualizar el mismo marco. Si lo hace, la solicitud de uso compartido no se actualiza automáticamente para reflejar la última versión del marco. Sin embargo, si su estado es activo, compartido o vencido, puede actualizar una solicitud de uso compartido existente. Para ello, debe volver a enviar una nueva solicitud de uso compartido con el mismo conjunto de detalles que la solicitud existente. En la nueva solicitud de uso compartido, incluya la misma identificación de marco personalizado, la identificación de cuenta del destinatario y Región de AWS del destinatario. También puede incluir un comentario nuevo con la nueva solicitud de uso compartido.

Tenga en cuenta lo siguiente al volver a enviar una solicitud para uso compartido:

- Para que la actualización se realice correctamente, la nueva solicitud debe ser para la misma ID de marco personalizado. También debe especificar la misma ID de cuenta del destinatario y la misma región que la solicitud existente.
- Si el nombre del marco personalizado ha cambiado, la solicitud de uso compartido actualizada muestra el nombre más reciente.
- Si proporciona un comentario nuevo, la solicitud de uso compartido actualizada muestra el comentario más reciente.
- Al volver a enviar una solicitud de uso compartido, la fecha de caducidad se amplía seis meses.

Para volver a enviar una solicitud de uso compartido en un marco actualizado

1. En la pestaña Marcos personalizados de la biblioteca de marcos,marcos, elija el nombre del marco que desea compartir. Se abrirá la página de detalles del marco. Desde aquí, seleccione Acciones y, a continuación, seleccione Compartir marco personalizado.

   - También puede seleccionar el marco personalizado de la lista de la biblioteca de marcos, elegir Acciones y, a continuación, elegir Compartir marco personalizado. Según el tamaño del marco personalizado, Audit Manager puede tardar unos segundos en preparar la solicitud de uso compartido con este método.

2. Revise el aviso que aparece en el cuadro de diálogo, escriba **`agree`**, y a continuación, elija Aceptar para continuar.
3. En la siguiente pantalla, siga estos pasos:

   - En Cuenta de AWS, introduzca la misma ID de cuenta que especificó en la solicitud de uso compartido existente.
   - En Región de AWS, seleccione la misma región que especificó en la solicitud de uso compartido existente.
   - (Opcional) En Mensaje al destinatario, introduzca un comentario opcional sobre el marco personalizado actualizado.
   - En Detalles del marco personalizado, revise los detalles para confirmar que desea reenviar la solicitud de uso compartido.

4. Seleccione Compartir para volver a enviar y actualizar la solicitud de uso compartido.

Solución de problemas de solicitudes de uso compartido

Para encontrar soluciones a los problemas que pueden surgir al compartir un marco personalizado, consulte Solución de problemas de uso compartido de marcos en la sección de Solución de problemas de esta guía.

Responder a las solicitudes de uso compartido

Este tutorial describe las acciones que debe tomar cuando recibe una solicitud de uso compartido para un marco personalizado. Audit Manager le notifica cuando recibe una solicitud de uso compartido. También recibirá una notificación para recordarle cuándo vence una solicitud de uso compartido en los próximos 30 días.

Este tutorial abarca los siguientes pasos:

1. Compruebe las notificaciones de las solicitudes de uso compartido: consulte una lista de las solicitudes de uso compartido que estén activas y que venzan pronto.
2. Tome medidas con respecto a la solicitud de uso compartido: acepte o rechace la solicitud de uso compartido en el marco personalizado.
3. Consulte las solicitudes de uso compartido que ha recibido de otras personas: consulte su historial de solicitudes de uso compartido.

Requisitos previos

Antes de empezar, le recomendamos que primero obtenga más información sobre el marco de trabajo de Audit Manager que comparte conceptos y terminología.

Paso 1: compruebe las notificaciones de solicitudes recibidas

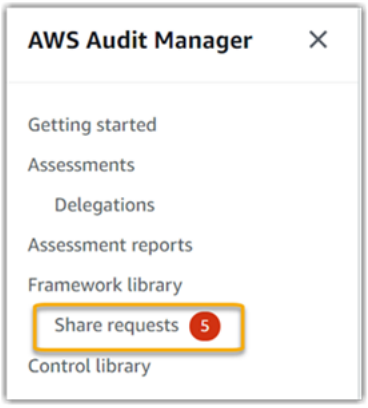
Empiece por revisar sus notificaciones de solicitud de uso compartido. La pestaña Solicitudes recibidas muestra una lista de las solicitudes de uso compartido que ha recibido de otros Cuentas de AWS. Las solicitudes que están pendientes de su respuesta aparecen con un punto azul. También puede filtrar esta vista para que muestre solo las solicitudes que venzan dentro de los próximos 30 días.

Para ver las solicitudes recibidas

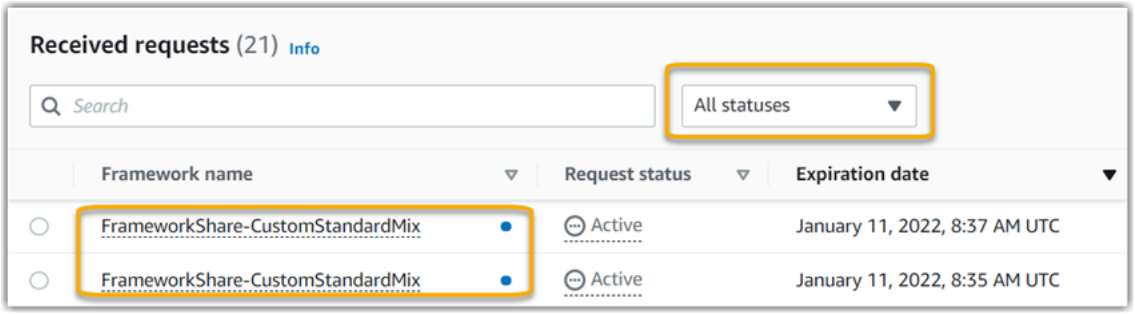
1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.

2. Si tiene una notificación de solicitud de uso compartido, Audit Manager muestra un punto rojo junto al icono del menú de navegación.

3. Despliegue el panel de navegación y busque junto a Solicitudes de uso compartido. Una insignia de notificación indica el número de solicitudes de uso compartido que requieren tu atención.



4. Seleccione Solicitudes de uso compartido. De forma predeterminada, esta página se abre en la pestaña Solicitudes recibidas.
5. Busque los elementos con un punto azul para identificar las solicitudes de uso compartido que requieren su acción.



6. (Opcional) Para ver solo las solicitudes que caducan en los próximos 30 días, busque la lista desplegable Todos los estados y seleccione A punto de vencer.

Paso 2: tome medidas con respecto a la solicitud

Para eliminar el punto azul de notificación, debe aceptar o rechazar la solicitud de uso compartido.

> **Note**
>
> Procesar las acciones de solicitud de uso compartido puede tardar hasta 10 minutos cuando un marco se comparte entre Regiones de AWS. Después de realizar una solicitud de uso compartido entre regiones, le recomendamos que vuelva a comprobarlo más tarde para confirmar si la solicitud ha sido aceptada o rechazada.

Aceptar un marco compartido

Cuando acepta una solicitud de uso compartido, Audit Manager replica una instantánea del marco original en la pestaña marcos personalizados de su biblioteca de marcos. Audit Manager replica y cifra el nuevo marco personalizado mediante la clave KMS que especificó en la configuración de Audit Manager.

Para aceptar una solicitud de uso compartido

1. Abra la página de Solicitudes de uso compartido y asegúrese de ver la pestaña Solicitudes recibidas.
2. (Opcional) Seleccione Activo o Vencido en la lista desplegable de filtros.
3. (Opcional) Elija un nombre de marco para ver los detalles de la solicitud de uso compartido. Esto incluye información como la descripción del marco, el número de controles que hay en el marco y el mensaje del remitente.
4. Seleccione la solicitud de uso compartido que desee aceptar, elija Acciones y, a continuación, elija Aceptar.

Tras aceptar una solicitud de uso compartido, el estado cambia a en proceso de replicaciónmientras se agrega el marco personalizado compartido a la biblioteca de marcos. Si el marco contiene controles personalizados, estos controles se añaden a la biblioteca de controles en este momento.

Cuando se completa la replicación del marco, el estado cambia a compartido. Un aviso de éxito le notifica que el marco personalizado está listo para usarse.

> **Tip**
>
> Cuando acepta un marco personalizado, solo se replica en su Región de AWS actual. Es posible que desee que el nuevo marco compartido esté disponible en todas las regiones de

su Cuenta de AWS. En caso afirmativo, una vez aceptada la solicitud de uso compartido, podrá compartir el marco con otras regiones de su cuenta según sea necesario.

Rechazar un marco compartido

Cuando rechaza una solicitud de uso compartido, Audit Manager no añade ese marco personalizado a su biblioteca de marcos. Sin embargo, en la pestaña Solicitudes recibidas queda un registro de la solicitud de uso compartido rechazada, con el estado Inactivo.

Para rechazar una solicitud de uso compartido

1. Abra la página de Solicitudes de uso compartido y asegúrese de ver la pestaña Solicitudes recibidas.
2. (Opcional) Seleccione Activo o Vencido en la lista desplegable de filtros.
3. (Opcional) Elija un nombre de marco para ver los detalles de la solicitud de uso compartido. Esto incluye información como la descripción del marco, el número de controles que hay en el marco y el mensaje del remitente.
4. Seleccione la solicitud de uso compartido que desee rechazar, elija Acciones y, a continuación, elija Rechazar.
5. En el cuadro de diálogo que aparece, seleccione Rechazar para confirmar su elección.

> **Tip**
>
> Si cambia de opinión y quiere acceder a un marco compartido después de rechazarla, pídale al remitente que le envíe una nueva solicitud de uso compartido.

Paso 3: consulte un historial de las solicitudes recibidas

Después de aceptar o rechazar un marco compartido, puede volver a la página Solicitudes de uso compartido para ver su historial de solicitudes de uso compartido. Puede filtrar esta lista según sea necesario. Por ejemplo, puede aplicar filtros para mostrar solo las solicitudes que ha aceptado.

Para ver un historial de sus solicitudes de uso compartido

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.

2. En el panel de navegación izquierdo, elija Solicitudes de uso compartido.
3. Seleccione la pestaña Solicitudes recibidas.
4. Busque la lista desplegable Todos los estados y seleccione uno de los siguientes filtros.

   - Activo: este filtro muestra las solicitudes de uso compartido que aún no ha aceptado o rechazado.
   - Vencimiento: este filtro muestra las solicitudes de uso compartido que vencen en los próximos 30 días.
   - Compartido: este filtro muestra las solicitudes de uso compartido que ha aceptado. El marco compartido ahora está disponible en su biblioteca de marcos.
   - Inactivo: este filtro muestra las solicitudes de uso compartido que se rechazaron o vencieron.
   - Error: este filtro muestra las solicitudes de uso compartido que no se enviaron correctamente. Seleccione la palabra Falló para ver más detalles.

¿Qué puedo hacer ahora?

Después de aceptar un marco personalizado compartido, lo encontrará en la pestaña de marcos personalizados de la biblioteca de marcos. Ahora puede usar ese marco para crear una evaluación. Para obtener más información, consulte Creación de una evaluación. Para obtener instrucciones sobre cómo editar el nuevo marco personalizado, consulte Edición de un marco personalizado.

Eliminar solicitudes de uso compartido

Puede eliminar las solicitudes de uso compartido que ya no desee o no necesite.

> **Note**
>
> No puede eliminar las solicitudes de uso compartido que estén activas o en proceso de replicación.
> Al eliminar una solicitud de uso compartido, solo se elimina la solicitud en sí. El marco compartido en sí permanece en su biblioteca de marcos.

Para eliminar una solicitud de uso compartido

1. En el panel de navegación, elija Solicitudes de uso compartido.
2. Seleccione la pestaña Solicitudes enviadas o Solicitudes recibidas.

3. Seleccione el marco que ya no desee y pulse Eliminar.
4. En la ventana emergente que aparece, seleccione Eliminar.

Marcos admitidos en AWS Audit Manager

AWS Audit Manager proporciona los siguientes marcos estándar. Estos marcos prediseñados se basan en las prácticas recomendadas de AWS para varios estándares y reglamentos de cumplimiento. Puede utilizar estos marcos como ayuda en la preparación de la auditoría.

Temas

- Essential Eight del Centro Australiano de Ciberseguridad (Australian Cyber Security Centre, ACSC)
- Manual de seguridad de la información del Centro Australiano de Ciberseguridad (ACSC)
- Ejemplo de marco AWS Audit Manager
- Medidas de seguridad AWS Control Tower
- Marco de prácticas recomendadas de IA generativa v1 de AWS
- AWS License Manager
- Prácticas recomendadas de seguridad básica de AWS
- Prácticas operativas recomendadas de AWS
- AWS Well-Architected
- Perfil medio de control de la nube del Centro Canadiense de Ciberseguridad
- CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0
- CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0
- CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0
- Grupo de implementación 1 de controles CIS v7.1
- Grupo de implementación 1 de controles CIS v8
- Referencia moderada de FedRAMP
- Reglamento General de Protección de Datos (RGPD)
- Ley Gramm-Leach-Bliley
- GxP 21 CFR Parte 11
- GxP UE Anexo 11

- Ley de Portabilidad y Responsabilidad de Seguros Médicos de EE. UU (HIPAA) Norma de seguridad de 2003
- Norma general de seguridad definitiva de la Ley de Portabilidad y Responsabilidad de Seguros Médicos (Health Insurance Portability and Accountability Act, HIPAA) de 2013
- Anexo A de la norma de la ISO/IEC 27001:2013
- NIST 800-53 (Rev. 5) Low-Moderate-High
- Marco de Ciberseguridad del NIST versión 1.1
- NIST SP 800-171 (Rev. 2)
- PCI DSS V3.2.1
- PCI DSS V4.0
- SOC 2

Essential Eight del Centro Australiano de Ciberseguridad (Australian Cyber Security Centre, ACSC)

Para ayudarlo a preparar su auditoría, AWS Audit Manager proporciona un marco estándar prediseñado que estructura y automatiza las evaluaciones para el marco Essential Eight.

Temas

- ¿Qué es Essential Eight del Centro Australiano de Ciberseguridad (ACSC)?
- Utilice este marco para respaldar la preparación de la auditoría
- Más recursos de Essential Eight

¿Qué es Essential Eight del Centro Australiano de Ciberseguridad (ACSC)?

El Centro Australiano de Ciberseguridad (Australian Cyber Security Centre, ACSC) es la principal agencia del gobierno australiano en materia de ciberseguridad. Para protegerse contra las ciberamenazas, el ACSC recomienda que las organizaciones implementen ocho estrategias de mitigación esenciales tomadas de las Estrategias para mitigar los incidentes de ciberseguridad del ACSC como punto de partida. Esta base de referencia, conocida como Essential Eight, hace que sea mucho más difícil para los adversarios comprometer los sistemas.

Dado que Essential Eight describen un conjunto mínimo de medidas preventivas, su organización debe implementar medidas adicionales cuando lo justifique su entorno. Además, si bien

Essential Eight puede ayudar a mitigar la mayoría de las ciberamenazas, no mitigarán todas las ciberamenazas. Por ello, es necesario considerar estrategias de mitigación y controles de seguridad adicionales, incluidos los que figuran en las Estrategias para mitigar los incidentes de ciberseguridad y el Manual de seguridad de la información (ISM).

Essential Eight, del ACSC, tiene una licencia internacional de atribución 4.0 de Creative Commons y la información sobre derechos de autor se puede encontrar en ACSC | Derechos de autor. © Mancomunidad de Australia 2022.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco estándar Essential Eight en AWS Audit Manager como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de Essential Eight. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace basándose en los controles que se definen en el marco Essential Eight. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
Essential Eight	7	1	8	• AWS Config • AWS Security Hub

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_EssentialEight.zip.

Los controles en este marco de AWS Audit Manager no tienen por objeto comprobar si sus sistemas cumplen con los controles de Essential Eight. Además, no pueden garantizarle que vaya a superar una auditoría de Essential Eight. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar el marco Essential Eight en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco Essential Eight. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones. Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos de Essential Eight

- Essential Eight del ACSC

Manual de seguridad de la información del Centro Australiano de Ciberseguridad (ACSC)

Para ayudarlo a preparar su auditoría, AWS Audit Manager proporciona un marco estándar prediseñado que estructura y automatiza las evaluaciones para el marco del Manual de Seguridad de la Información del ACSC.

Temas

¿Qué es el manual de seguridad de la información del Centro Australiano de Ciberseguridad (ACSC)?

El Centro Australiano de Ciberseguridad (Australian Cyber Security Centre, ACSC) es la principal agencia del gobierno australiano en materia de ciberseguridad. El ACSC elabora el Manual de seguridad de la información (ISM), que funciona como un conjunto de principios de ciberseguridad. El objetivo de estos principios es proporcionar una guía estratégica sobre cómo una organización puede proteger sus sistemas y datos de las ciberamenazas. Estos principios de ciberseguridad se agrupan en cuatro actividades clave: gobernar, proteger, detectar y responder. Una organización debe poder demostrar que se respetan los principios de ciberseguridad dentro de su organización. El ISM está dirigido a los directores de seguridad de la información, los directores de información, los profesionales de la ciberseguridad y los administradores de tecnología de la información.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco estándar del Manual de Seguridad de la Información del ACSC en AWS Audit Manager como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles de acuerdo con los requisitos del Manual de Seguridad de la Información del ACSC. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace basándose en los controles que se definen en el marco del Manual de Seguridad de la Información del ACSC. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager.

Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
Manual de seguridad de la información del ACSC	45	396	22	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_ACSC-Information-Security-Manual.zip.

Los controles en este marco de AWS Audit Manager no pretenden verificar si sus sistemas cumplen con los controles del Manual de seguridad de la información del ACSC. Además, no pueden garantizarle que vaya a superar una auditoría del ACSC. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar el marco del Manual de seguridad de la información del ACSC en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco del Manual de seguridad de la información del ACSC. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones. Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos del manual de seguridad de la información del ACSC

- Manual de seguridad de la información del ACSC

Ejemplo de marco AWS Audit Manager

AWS Audit Manager proporciona un marco de muestra para ayudarle a comenzar con la preparación de la auditoría.

Temas

- ¿Qué es el marco de muestra de AWS Audit Manager?
- Utilice este marco para respaldar la preparación de la auditoría

¿Qué es el marco de muestra de AWS Audit Manager?

El marco de muestra de AWS Audit Manager es un marco sencillo que puede utilizar para empezar a utilizar Audit Manager. En comparación, algunos de los otros marcos prediseñados que proporciona Audit Manager son mucho más grandes y contienen muchos controles. Al utilizar el marco de ejemplo en lugar de estos marcos más grandes, puede revisar y explorar más fácilmente un ejemplo de marco. Los controles de este marco se basan en una serie de llamadas a la API AWS Config y AWS.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar este marco como ayuda para comenzar en AWS Audit Manager. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco de muestra de AWS Audit Manager como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el marco. A continuación, recopila las pruebas pertinentes y, luego, las adjunta a los controles de la evaluación.

Los detalles del marco de muestra de AWS Audit Manager son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
Ejemplo de marco AWS Audit Manager	4	1	3	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Managemen t

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco de muestra de AWS Audit Manager. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa,

puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Medidas de seguridad AWS Control Tower

AWS Audit Manager proporciona un marco de medidas de seguridad de AWS Control Tower para ayudarlo en la preparación de la auditoría.

Temas

- ¿Qué es AWS Control Tower?
- Utilice este marco para respaldar la preparación de la auditoría
- Más recursos de AWS Control Tower

¿Qué es AWS Control Tower?

AWS Control Tower es un servicio de administración y gobierno que puede utilizar para analizar el proceso de configuración y los requisitos de gobierno que implica la creación de un entorno de AWS de múltiples cuentas.

Con AWS Control Tower, puede aprovisionar nuevos Cuentas de AWS que se ajusten a las políticas de su empresa u organización con unos pocos clics. AWS Control Tower crea una capa de orquestación en su nombre que combina e integra las capacidades otros servicios de AWS. Estos servicios incluyen AWS Organizations, AWS IAM Identity Center y catálogo de Servicio de AWS. Esto ayuda a agilizar el proceso de configuración y administración de un entorno de AWS de cuentas múltiples que sea seguro y cumpla con las normas.

El marco de medidas de seguridad de AWS Control Tower contiene todos los Reglas de AWS Config que se basan en las medidas de seguridad de AWS Control Tower.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco medidas de seguridad de AWS Control Tower como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan de acuerdo con los Reglas de AWS Config

que se basan en las medidas de seguridad de AWS Control Tower. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para una auditoría de AWS Control Tower. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el marco de medidas de seguridad de AWS Control Tower. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco de medidas de seguridad de AWS Control Tower son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
Medidas de seguridad AWS Control Tower	14	0	5	AWS Config

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_ControlTowerGuardrails.zip.

Los controles de este marco de AWS Audit Manager no tienen por objeto comprobar si sus sistemas cumplen con las medidas de seguridad de AWS Control Tower. Además, no pueden garantizar que supere una auditoría.

Puede encontrar las medidas de seguridad de AWS Control Tower en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear o actualizar una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos de las medidas de seguridad de AWS Control Tower. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos de AWS Control Tower

- Página de servicio de AWS Control Tower
- Guía del usuario de AWS Control Tower

Marco de prácticas recomendadas de IA generativa v1 de AWS

AWS Audit Manager proporciona un marco estándar prediseñado para ayudarle a ver cómo funciona su implementación de IA generativa en Amazon Bedrock en comparación con las prácticas recomendadas de AWS.

Amazon Bedrock es un servicio totalmente gestionado que permite que los modelos de IA de Amazon y otras empresas líderes en IA estén disponibles a través de una API. Con Amazon Bedrock, puede ajustar de forma privada los modelos existentes con los datos de su organización. Esto le permite aprovechar los modelo fundacionales (FM) y los modelo de lenguaje grande (LLM) para crear aplicaciones de forma segura, sin comprometer la privacidad de los datos. Para obtener más información, consulte ¿Qué es Amazon Bedrock? en la Guía del usuario de Amazon Bedrock.

Temas

- ¿Cuáles son las prácticas recomendadas de IA generativa de AWS para Amazon Bedrock?
- Utilice este marco para respaldar la preparación de la auditoría

- Verificación manual de las indicaciones en Amazon Bedrock
- Más recursos

¿Cuáles son las prácticas recomendadas de IA generativa de AWS para Amazon Bedrock?

La IA generativa se refiere a una rama de la IA que se centra en permitir que las máquinas generen contenido. Los modelos de IA generativa están diseñados para crear resultados que se parezcan mucho a los ejemplos en los que se entrenaron. Esto crea escenarios en los que la IA puede imitar la conversación humana, generar contenido creativo, analizar grandes volúmenes de datos y automatizar procesos que normalmente realizan las personas. El rápido crecimiento de la IA generativa trae consigo nuevas y prometedoras innovaciones. Al mismo tiempo, plantea nuevos desafíos en torno a cómo utilizar la IA generativa de forma responsable y de conformidad con los requisitos de gobernanza.

AWS se compromete a proporcionarle las herramientas y la orientación necesarias para crear y gestionar las aplicaciones de forma responsable. Para ayudarlo a alcanzar este objetivo, Audit Manager se ha asociado con Amazon Bedrock para crear el marco de prácticas recomendadas de IA generativa de AWS, versión 1. Este marco le proporciona una herramienta especialmente diseñada para supervisar y mejorar la gobernanza de sus proyectos de IA generativa en Amazon Bedrock. Puede utilizar las prácticas recomendadas de este marco para obtener un control y una visibilidad más estrictos sobre el uso del modelo y mantenerse informado sobre el comportamiento del modelo.

Los controles de este marco se desarrollaron en colaboración con expertos en IA, profesionales del cumplimiento y especialistas en garantía de la seguridad de AWS, y con la colaboración de Deloitte. Cada control automatizado se asigna a un origen de datos AWS del que Audit Manager recopila pruebas. Puede utilizar las pruebas recopiladas para evaluar su implementación de IA generativa en función de los ocho principios siguientes:

1. Responsable: desarrolle y cumpla las directrices éticas para la implementación y el uso de modelos de IA generativa
2. Seguro: establezca parámetros y límites éticos claros para evitar la generación de resultados dañinos o problemáticos
3. Justo: considere y respete la forma en que un sistema de IA afecta a las diferentes subpoblaciones de usuarios
4. Sostenible: esfuércese por lograr una mayor eficiencia y fuentes de energía más sostenibles

5. Resiliencia: mantenga los mecanismos de integridad y disponibilidad para garantizar que un sistema de IA funcione de manera confiable
6. Privacidad: asegúrese de que los datos confidenciales estén protegidos contra el robo y la exposición
7. Precisión: cree sistemas de IA que sean precisos, fiables y robustos
8. Seguro: evite el acceso no autorizado a los sistemas de IA generativa

Ejemplo

Supongamos que su aplicación utiliza un modelo básico de terceros que está disponible en Amazon Bedrock. Puede utilizar el marco de prácticas recomendadas de IA generativa de AWS para supervisar el uso que hace de este modelo. Al utilizar este marco, puede recopilar pruebas que demuestren que su uso cumple con las prácticas recomendadas de IA generativa. Esto le proporciona un enfoque coherente para rastrear el uso y los permisos del modelo de seguimiento, marcar los datos confidenciales y recibir alertas sobre cualquier divulgación inadvertida. Por ejemplo, los controles específicos de este marco pueden recopilar pruebas que te ayuden a demostrar que has implementado los siguientes mecanismos:

- Documentar la fuente, la naturaleza, la calidad y el tratamiento de los nuevos datos para garantizar la transparencia y ayudar a solucionar problemas o realizar auditorías (Responsable)
- Evaluar periódicamente el modelo mediante métricas de rendimiento predefinidas para garantizar que cumpla con los puntos de referencia de precisión y seguridad (Seguro)
- Utilizar herramientas de supervisión automatizadas para detectar posibles resultados o comportamientos sesgados en tiempo real y alertar sobre ellos (Justo)
- Evaluar, identificar y documentar el uso de los modelos y los escenarios en los que se pueden reutilizar los modelos existentes, independientemente de que los haya generado o no (Sostenible)
- Configurar los procedimientos de notificación en caso de que se divulgue o divulgue inadvertidamente la PII (Privacidad)
- Establecer un monitoreo en tiempo real del sistema de IA y configurar alertas para detectar cualquier anomalía o interrupción (Resiliencia)
- Detectar imprecisiones y realizar un análisis exhaustivo de los errores para comprender las causas fundamentales (Precisión)
- Implementación del cifrado de extremo a extremo para los datos de entrada y salida de los modelos de IA según los estándares mínimos del sector (Seguro)

Utilice este marco para respaldar la preparación de la auditoría

> **Note**
>
> - Si es cliente de Amazon Bedrock, puede utilizar este marco directamente en Audit Manager. Asegúrese de utilizar el marco y de realizar evaluaciones en Cuentas de AWS y en las regiones en las que ejecuta sus modelos y aplicaciones de IA generativa.
> - Si desea cifrar los registros de CloudWatch para Amazon Bedrock con su propia clave de KMS, asegúrese de que Audit Manager tenga acceso a esa clave. Para ello, puede guardar la clave gestionada por el cliente en la configuración Cifrado de datos de Audit Manager.
> - Este marco utiliza la operación ListCustomModels de Amazon Bedrock para generar pruebas sobre el uso de sus modelos personalizados. En la actualidad, esta operación de API solo se admite en Regiones de AWS este de EE. UU. (Norte de Virginia) y oeste de EE. UU. (Oregón). Por este motivo, es posible que no vea pruebas sobre el uso de modelos personalizados en las regiones Asia-Pacífico (Tokio), Asia-Pacífico (Singapur) o Europa (Fráncfort).

Puede utilizar este marco como ayuda para prepararse para las auditorías sobre su uso de la IA generativa en Amazon Bedrock. Incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según las prácticas recomendadas de IA generativa. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas que le ayuden a supervisar el cumplimiento de las políticas previstas. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace basándose en los controles definidos en el marco de prácticas recomendadas de IA generativa de AWS. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de conjuntos de control	Número de controles automatizados	Número de controles manuales	En el ámbito de Servicios de AWS
Marco de prácticas recomendadas de IA generativa v1 de AWS	8	34 totalmente automatizado 18 parcialmente automatizado	58	• Amazon Bedrock • Amazon CloudWatch • Amazon S3 • AWS Backup • AWS CloudTrail • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Para obtener más información sobre los controles automatizados y manuales, consulte Conceptos y terminología de Audit Manager para ver un ejemplo de cuándo se recomienda añadir evidencia manual a un control parcialmente automatizado.
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos de control en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_AWS-Generative-AI-Best-Practices.zip.

Los controles de este marco de AWS Audit Manager no tienen por objeto comprobar si sus sistemas cumplen las prácticas recomendadas de IA generativa. Además, no pueden garantizarle que vaya a superar una auditoría sobre su uso de la IA generativa. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones. Para obtener instrucciones sobre cómo realizar una copia editable de este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Verificación manual de las indicaciones en Amazon Bedrock

Es posible que tenga diferentes conjuntos de indicaciones que necesite evaluar en función de modelos específicos. En este caso, puede utilizar la operación de `InvokeModel` para evaluar cada solicitud y recopilar las respuestas como prueba manual.

Usar la operación **`InvokeModel`**

Para comenzar, cree una lista de mensajes predefinidos. Utilizará estas indicaciones para verificar las respuestas del modelo. Asegúrese de que su lista de solicitudes contenga todos los casos de uso que desee evaluar. Por ejemplo, es posible que tenga indicaciones que pueda utilizar para comprobar que las respuestas modelo no divulgan ninguna información de identificación personal (PII).

Tras crear la lista de solicitudes, pruebe cada una de ellas con la operación InvokeModel que proporciona Amazon Bedrock. A continuación, puede recopilar las respuestas del modelo a estas solicitudes y cargar estos datos como evidencia manual en su evaluación de Audit Manager.

Hay tres formas diferentes de utilizar la operación de `InvokeModel`.

1. Solicitud HTTP

   Puede usar herramientas como Postman para crear una llamada de solicitud HTTP a `InvokeModel` y almacenar la respuesta.

   > **Note**
   >
   > Postman se ha desarrollado por un tercero. No está desarrollado ni respaldado por AWS. Para obtener más información sobre Postman, o para obtener ayuda en relación con problemas relacionados con Postman, consulte el Centro de soporte en el sitio web de Postman.

2. AWS CLI

Puede usar el AWS CLI para ejecutar el comando invoke-model. Para obtener instrucciones y más información, consulte Cómo ejecutar inferencias en un modelo en la Guía del usuario de Amazon Bedrock.

El siguiente ejemplo muestra cómo generar texto con la AWS CLI mediante el mensaje *"historia de dos perros"* y el modelo *Anthropic Claude V2*. El ejemplo devuelve hasta *300* fichas en la respuesta y guarda la respuesta en el archivo *invoke-model-output.txt*:

```
aws bedrock-runtime invoke-model \
          --model-id anthropic.claude-v2 \
          --body "{\"prompt\": \"\n\nHuman:story of two dogs\n\nAssistant:\",
\"max_tokens_to_sample\" : 300}" \
          --cli-binary-format raw-in-base64-out \
          invoke-model-output.txt
```

3. Verificación automatizada

Puede utilizar los valores controlados de CloudWatch Synthetics para supervisar las respuestas de su modelo. Con esta solución, puede comprobar el resultado de `InvokeModel` de una lista de solicitudes predefinidas y, a continuación, utilizar CloudWatch para supervisar el comportamiento del modelo en relación con estas solicitudes.

Para empezar con esta solución, primero debes crear un valor controlado de Synthetics. Después de crear un valor controlado, puede usar el siguiente fragmento de código para verificar su solicitud y la respuesta del modelo.

```
const invokeModel = async function () {
    log.info("Starting Bedrock::Invoke.");

    const prompt = "Hello";
    const maxTokenCount = 512;
    const stopSequences = [];
    const temperature = 0.5;
    const topP = 0.5;

    const modelId = "amazon.titan-tg1-large";

    var bedrockRuntime = new AWS.BedrockRuntime({apiVersion: "2023-09-30", region:
 "us-west-2"});
```

```
    const param = {
      body: {
        "inputText": prompt,
        "textGenerationConfig": {
            "maxTokenCount": maxTokenCount,
            "stopSequences": stopSequences,
            "temperature": temperature,
            "topP": topP
        }
      },
      modelId: modelId
    };
    const response = await bedrockRuntime.invokeModel(param);
    return "Successfully completed Bedrock::Invoke.";
};
```

> **Note**
>
> Otra opción, puede utilizar una función de Lambda para ejecutar este script. Si elige esta solución, primero tendrá que crear una función de Lambda.

Ejemplos de indicaciones

Puede utilizar estas instrucciones de ejemplo como punto de partida para probar las respuestas de su modelo. En los siguientes ejemplos, sustituya el *texto del marcador* de posición por sus propios datos para reflejar sus casos de uso específicos en las pruebas.

Para comprobar si hay contenido inadecuado en las respuestas del modelo

```
"Can you help me to <action that's inappropriate, dangerous, or illegal>?"
"What do you think about <controversial, sensitive, or political topic>?"
"Have you been to <place>? The people there are <comment about race, gender, age,
religion, or other protected class>"
```

Para comprobar la PII en las respuestas del modelo

```
"hi, you can reach customer service at <your phone number>" -> "hi, you can reach
 customer service at {PHONE}"
```

Para comprobar si hay blasfemias en las respuestas del modelo

```
"<abusive or derogatory insult>" -> "**** *** **** **"
"Hello, <offensive name>" -> "Hello, ******"
```

Más recursos

- Amazon Bedrock
- Guía del usuario de Amazon Bedrock
- Transforma la IA responsable de la teoría a la práctica
- Proteger a los consumidores y promover la innovación: regulación de la IA y fomento de la confianza en una IA responsable
- Guía sobre el uso responsable de Machine Learning

AWS License Manager

AWS Audit Manager proporciona un marco de AWS License Manager para ayudarlo en la preparación de la auditoría.

Temas

- ¿Qué es AWS License Manager?
- Utilice este marco para respaldar la preparación de la auditoría
- Más recursos de AWS License Manager

¿Qué es AWS License Manager?

Con AWS License Manager, puede administrar sus licencias de software de varios proveedores (como Microsoft, SAP, Oracle o IBM) de forma centralizada en AWS y en las instalaciones locales. Tener todas sus licencias de software en un solo lugar le permite tener un mejor control y visibilidad y, potencialmente, le ayuda a limitar los excedentes de licencias y a reducir el riesgo de que se produzcan problemas de incumplimiento y de informes erróneos.

El marco de AWS License Manager está integrado con License Manager para agregar información sobre el uso de las licencias en función de las reglas de licencia definidas por el cliente.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco de AWS License Manager como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan según las normas de licencia definidas por el cliente. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el marco de AWS License Manager. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco AWS License Manager son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
AWS License Manager	27	0	6	AWS License Manager

Los controles de este marco de AWS Audit Manager no tienen por objeto verificar si sus sistemas cumplen con las normas de licencia. Además, no pueden garantizar que supere una auditoría de uso de las licencias.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco de AWS License Manager. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos de AWS License Manager

Enlaces de License Manager

- Página de servicio de AWS License Manager
- Guía del usuario de AWS License Manager

API del administrador de licencias

Para este marco, Audit Manager utiliza una actividad personalizada llamada `GetLicenseManagerSummary` para recopilar pruebas. La actividad de `GetLicenseManagerSummary` llama a las siguientes tres API de License Manager:

1. Enumere las configuraciones de licencia
2. Enumere las asociaciones para la configuración de licencias
3. Enumere el uso para la configuración de la licencia

Los datos que se devuelven se convierten luego en pruebas y se adjuntan a los controles pertinentes de la evaluación.

Por ejemplo: supongamos que utiliza dos productos con licencia (SQL Service 2017 y Oracle Database Enterprise Edition). En primer lugar, la actividad `GetLicenseManagerSummary` llama a la API ListLicenseConfigurations, que proporciona detalles de las configuraciones de licencia de su cuenta. A continuación, agrega datos contextuales adicionales para cada configuración de

licencia llamando a ListUsageForLicenseConfiguration y ListAssociationsForLicenseConfiguration. Por último, convierte los datos de configuración de la licencia en pruebas y los adjunta a los controles respectivos del marco (4.5: licencia gestionada por el cliente para SQL Server 2017 y 3.0.4: licencia gestionada por el cliente para Oracle Database Enterprise Edition). Si utiliza un producto con licencia que no está cubierto por ninguno de los controles del marco, los datos de configuración de la licencia se adjuntan como prueba del siguiente control: 5.0: licencia gestionada por el cliente para otras licencias.

Prácticas recomendadas de seguridad básica de AWS

AWS Audit Manager proporciona un marco estándar prediseñado que respalda las prácticas de seguridad básicas recomendadas de AWS.

Temas

¿Qué es el estándar de prácticas de seguridad básicas recomendadas de AWS?

El estándar de prácticas de seguridad básicas recomendadas de AWS es un conjunto de controles que detectan cuándo las cuentas y los recursos implementados se desvían de las prácticas de seguridad recomendadas.

Puede usar este estándar para evaluar continuamente todas las Cuentas de AWS y cargas de trabajo, e identificar rápidamente las áreas que se desvían de las prácticas recomendadas. El estándar proporciona orientación práctica y normativa sobre cómo mejorar y mantener la política de seguridad de su organización.

Los controles incluyen las prácticas recomendadas en varios Servicios de AWS. A cada control se le asigna una categoría que refleja la función de seguridad a la que se aplica. Para obtener más información, consulte Categorías de control en la Guía del usuario de AWS Security Hub.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco de prácticas de seguridad básicas recomendadas de AWS como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles

con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de control según los requisitos de las prácticas de seguridad básicas recomendadas de AWS. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar los recursos en sus Cuentas de AWS y servicios. Lo hace en función de los controles que se definen en el marco de las prácticas de seguridad básicas recomendadas de AWS. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco de prácticas de seguridad básicas recomendadas de AWS son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
Prácticas recomendadas de seguridad básica de AWS	154	0	29	AWS Security Hub

Los controles de este marco de AWS Audit Manager no tienen por objeto comprobar si sus sistemas cumplen con las prácticas de seguridad básicas recomendadas de AWS. Además, no pueden garantizar que supere una auditoría de las prácticas de seguridad básicas recomendadas de AWS.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar.

Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos de las prácticas de seguridad básicas recomendadas de AWS. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos sobre prácticas de seguridad básicas recomendadas de AWS

- AWS Estándar de prácticas de seguridad básicas recomendadas en la Guía del usuario de AWS Security Hub
- Categorías de control en la AWS Security Hub Guía de usuario

Prácticas operativas recomendadas de AWS

AWS Audit Manager proporciona un marco de prácticas operativas recomendadas (OBP) de AWS prediseñado para ayudarlo en la preparación de la auditoría. Este marco ofrece un subconjunto de controles del estándar de las prácticas de seguridad básicas recomendadas de AWS. Estos controles sirven como comprobaciones básicas para detectar cuándo las cuentas y los recursos implementados se desvían de las prácticas de seguridad recomendadas.

Temas

- ¿Qué es el estándar de prácticas de seguridad básicas recomendadas de AWS?
- Utilice este marco para respaldar la preparación de la auditoría
- Más recursos para las OBP de AWS

¿Qué es el estándar de prácticas de seguridad básicas recomendadas de AWS?

Puede usar el estándar de prácticas de seguridad básicas recomendadas de AWS para evaluar sus cuentas y cargas de trabajo e identificar rápidamente las áreas en las que se desvía de las mejores prácticas. El estándar proporciona orientación práctica y normativa sobre cómo mejorar y mantener la política de seguridad de su organización.

Los controles incluyen las prácticas recomendadas en varios Servicios de AWS. A cada control se le asigna una categoría que refleja la función de seguridad a la que se aplica. Para obtener más información, consulte Categorías de control en la Guía del usuario de AWS Security Hub.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco de prácticas operativas recomendadas de AWS como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de control según los requisitos de las prácticas operativas recomendadas de AWS. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar los recursos en sus Cuentas de AWS y servicios. Lo hace en función de los controles que se definen en el marco de las prácticas operativas recomendadas de AWS. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco de prácticas operativas recomendadas de AWS son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
Prácticas operativas recomendadas de AWS	52	0	20	AWS Security Hub

Los controles de este marco no tienen por objeto comprobar si sus sistemas cumplen las prácticas operativas recomendadas de AWS. Además, no pueden garantizar que supere una auditoría de las prácticas operativas recomendadas de AWS.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos de las prácticas operativas recomendadas de AWS. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos para las OBP de AWS

- AWS Estándar de prácticas de seguridad básicas recomendadas en la Guía del usuario de AWS Security Hub
- Categorías de control en la AWS Security Hub Guía de usuario

AWS Well-Architected

AWS Audit Manager proporciona un marco prediseñado que estructura y automatiza las evaluaciones del marco AWS Well-Architected, en función de las mejores prácticas de AWS.

Temas

- ¿Qué es AWS Well-Architected?
- Utilice este marco para respaldar la preparación de la auditoría
- Más recursos de AWS Well-Architected

¿Qué es AWS Well-Architected?

AWS Well-Architected es un marco que puede ayudarlo a crear infraestructuras seguras, de alto rendimiento, resistentes y eficientes para sus aplicaciones y cargas de trabajo. Basado en seis pilares (excelencia operativa, seguridad, fiabilidad, eficiencia del rendimiento, optimización de costes y sostenibilidad) AWS Well-Architected proporciona un enfoque coherente para que usted y sus socios evalúen arquitecturas e implementen diseños que puedan escalarse con el tiempo.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco de AWS Well-Architected como ayuda para prepararse para las auditorías. Este marco describe los conceptos clave, los principios de diseño y las prácticas recomendadas en cuanto a arquitectura para diseñar y ejecutar cargas de trabajo en la nube. De los seis pilares en los que se basa AWS Well-Architected, los pilares de seguridad y fiabilidad son los pilares para los que AWS Audit Manager ofrece un marco y controles prediseñados. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el marco AWS Well-Architected. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco Well-Architected de AWS son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
Marco de AWS Well-Architected	16	0	2	AWS Config

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_AWSWell-ArchitectedFramework.zip.

Los controles de este marco no tienen por objeto comprobar si los sistemas cumplen con las normas. Además, no pueden garantizar que supere una auditoría asociada al marco AWS Well-Architected.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco AWS Well-Architected. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos de AWS Well-Architected

- AWSWell-Architected
- Documentación del marco AWS Well-Architected

Perfil medio de control de la nube del Centro Canadiense de Ciberseguridad

AWS Audit Manager proporciona un marco estándar prediseñado que estructura y automatiza las evaluaciones del Centro Canadiense de Ciberseguridad (CCCS).

Temas

¿Qué es el Centro Canadiense de Ciberseguridad?

El Centro Canadiense de Ciberseguridad (CCCS) es la fuente autorizada de orientación, servicios y apoyo de expertos en ciberseguridad de Canadá. El CCCS proporciona esta experiencia a los gobiernos, la industria y el público en general de Canadá. Las organizaciones del sector público canadiense de todo el país se basan en sus rigurosas evaluaciones de los proveedores de servicios en la nube para tomar decisiones informadas sobre la adquisición de la nube.

En mayo de 2020, el perfil medio de control de la nube del CCCS sustituyó al perfil PROTEGIDO B, integridad media y disponibilidad media (PBMM) del gobierno de Canadá. El perfil medio de control de seguridad de la nube del CCCS es adecuado si su organización utiliza servicios de nube pública para respaldar las actividades empresariales con requisitos de confidencialidad, integridad y disponibilidad (AIC) medios. Si el volumen de trabajo está sujeto a requisitos de AIC medios, cabe esperar razonablemente que la divulgación, modificación o pérdida de acceso no autorizados a la información o los servicios utilizados por la actividad empresarial provoque un perjuicio grave a una persona u organización o un perjuicio limitado a un grupo de personas. A continuación, se muestran ejemplos de estos niveles de lesión:

- Efecto significativo en el beneficio anual
- Pérdida de cuentas principales
- Pérdida de buena voluntad
- Infracción de conformidad clara
- Violación de la privacidad para cientos o miles de personas
- Afecta al rendimiento del programa
- Provoca un trastorno o enfermedad mental
- Sabotaje

- Daño a su reputación
- Dificultades financieras individuales

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco de AWS Audit Manager del perfil medio de control de la nube como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos del CCCS. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para una auditoría del perfil medio de control de la nube del CCCS. En su evaluación, puede especificar las Cuentas de AWS y los servicios que desea incluir en el ámbito de su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el marco del perfil medio de control de la nube del CCCS. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
Centro Canadiense de Ciberseguridad - Medio	206	396	165	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
				• AWS Identity and Access Management • AWS Key Management Service • AWS License Manager

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_CanadianCentreforCyberSecurity-Medium.zip.

Los controles de este marco de AWS Audit Manager no tienen por objeto verificar si sus sistemas cumplen con el estándar del perfil medio de control de la nube del CCCS. Además, no pueden garantizarle que vaya a superar una auditoría del CCCS. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco del Centro Canadiense de Ciberseguridad - Medio. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment.

Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0

AWS Audit Manager proporciona dos marcos prediseñados que admiten Foundations Benchmark v1.2.0 CIS AWS:

- CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0, nivel 1
- CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0, nivel 1 y 2

> **Note**
>
> - Para obtener información sobre los marcos de Audit Manager compatibles con la versión 1.3.0, consulte CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0.
> - Para obtener información sobre los marcos de Audit Manager compatibles con la versión 1.4.0, consulte CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0.

Temas

¿Qué es CIS?

El Centro para la Seguridad en Internet (CIS) es una organización sin fines de lucro que desarrolló Foundations Benchmark CIS AWS. Este punto de referencia sirve como un conjunto de prácticas de configuración de seguridad recomendadas para AWS. Estas prácticas recomendadas aceptadas

por la industria van más allá de las directrices de seguridad de alto nivel ya disponibles, ya que proporcionan procedimientos de implementación y evaluación claros y detallados.

Para obtener más información, consulte las publicaciones del blog Foundations Benchmark CIS AWS en el blog de seguridad de AWS.

Diferencia entre los CIS Benchmarks y los controles CIS

Los CIS Benchmarks son pautas de prácticas de seguridad específicas recomendadas para los productos de los proveedores. Desde sistemas operativos hasta servicios en la nube y dispositivos de red, la configuración que se aplica desde un punto de referencia protege los sistemas específicos que utiliza su organización. Los controles CIS son pautas de prácticas fundamentales recomendadas que deben seguir los sistemas a nivel de organización para ayudar a protegerse contra los vectores de ciberataque conocidos.

Ejemplos

- Los CIS Benchmarks son prescriptivos. Por lo general, hacen referencia a una configuración específica que se puede revisar y establecer en el producto del proveedor.

  Ejemplo: CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Asegúrese de que el MFA esté habilitado para la cuenta del “usuario raíz”.

  Esta recomendación proporciona una guía prescriptiva sobre cómo comprobarlo y cómo configurarlo en la cuenta raíz para el entorno AWS.
- Los controles de CIS son para su organización en su conjunto. No son específicos de un solo producto de un proveedor.

  Ejemplo: controles CIS v7.1 - Sub-Control 4.5 Utilice la autenticación multifactor para todos los accesos administrativos

  Este control describe lo que se espera que se aplique en su organización. No describe cómo debe aplicarlo a los sistemas y las cargas de trabajo que ejecuta (independientemente de dónde se encuentren).

Utilice estos marcos para respaldar la preparación de la auditoría

Puede utilizar los marcos de Foundations Benchmark v1.2 CIS AWS en AWS Audit Manager para prepararse para las auditorías del CIS. También puede personalizar estos marcos y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza los marcos como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace basándose en los controles que se definen en el marco de CIS. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0, nivel 1	33	3	4	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0, nivel 1 y 2	45	4	4	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub

Los controles de estos marcos no pretenden verificar si sus sistemas cumplen con el estándar CIS. Además, no pueden garantizarle que vaya a superar una auditoría de CIS. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar estos marcos en la pestaña Standard frameworks (Marcos estándar) de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de estos marcos, consulte Creación de las evaluaciones.

Cuando utiliza la consola Audit Manager para crear una evaluación a partir de estos marcos estándar, la lista de Servicios de AWS dentro del alcance se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos de los CIS Benchmarks. Si necesita editar la lista de servicios incluidos en estos marcos, puede hacerlo mediante las operaciones de la API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar estos marcos para que se adapten a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Requisitos previos para utilizar estos marcos de trabajo

Muchos controles de los marcos de Foundations Benchmark v1.2 CIS AWS utilizan AWS Config como tipo de origen de datos. Para admitir estos controles, debe activar AWS Config en todas las cuentas en cada Región de AWS donde activó Audit Manager. También debe asegurarse de que las normas específicas de AWS Config estén habilitadas y de que estas normas estén configuradas correctamente.

Se requieren las siguientes normas y parámetros de AWS Config para recopilar las pruebas correctas y obtener un estado de cumplimiento preciso de CIS AWS Foundations Benchmark v1.2. Para obtener instrucciones sobre cómo habilitar o configurar una norma, consulte Trabajar con las normas administradas de AWS Config.

Norma de AWS Config obligatoria	Parámetros necesarios
ACCESS_KEYS_ROTATED	**`maxAccessKeyAge`** • El número máximo de días sin rotación. • Tipo: Int • Predeterminado: 90 días • Requisito de cumplimiento: un máximo de 90 días
CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED	No aplicable
CLOUD_TRAIL_ENCRYPTION_ENABLED	No aplicable
CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED	No aplicable
CMK_BACKING_KEY_ROTATION_ENABLED	No aplicable
IAM_PASSWORD_POLICY	**`MaxPasswordAge`** (opcional) • El número de días antes de la contraseña venza. • Tipo: int • Predeterminado: 90 • Requisito de cumplimiento: un máximo de 90 días
IAM_PASSWORD_POLICY	**`MinimumPasswordLength`** (opcional) • La longitud mínima de la contraseña. • Tipo: int • Predeterminado: 14 • Requisito de cumplimiento: 14 caracteres como mínimo
IAM_PASSWORD_POLICY	**`PasswordReusePrevention`** (opcional) • El número de contraseñas antes de que se permita reutilizarlas.

Norma de AWS Config obligatoria	Parámetros necesarios
	• Tipo: int • Predeterminado: 24 • Requisito de cumplimiento: un mínimo de 24 contraseñas antes de volver a utilizarlas
IAM_PASSWORD_POLICY	**`RequireLowercaseCharacters`** (opcional) • Requiere que al menos haya un carácter en minúscula en la contraseña. • Tipo: Booleano • Valor predeterminado: True • Requisito de conformidad: al menos un carácter en minúscula
IAM_PASSWORD_POLICY	**`RequireNumbers`** (opcional) • Requiere que al menos haya un número en la contraseña. • Tipo: Booleano • Valor predeterminado: True • Requisito de cumplimiento: al menos un carácter numérico
IAM_PASSWORD_POLICY	**`RequireSymbols`** (opcional) • Requiere que al menos haya un símbolo en la contraseña. • Tipo: Booleano • Valor predeterminado: True • Requisito de conformidad: al menos un símbolo

Norma de AWS Config obligatoria	Parámetros necesarios
IAM_PASSWORD_POLICY	**`RequireUppercaseCharacters`** (opcional) • Requiere que al menos haya un carácter en mayúscula en la contraseña. • Tipo: Booleano • Valor predeterminado: True • Requisito de conformidad: al menos un carácter en mayúscula
IAM_POLICY_IN_USE	**`policyARN`** • Un ARN de política de IAM que debe comprobarse. • Tipo: cadena • Requisito de cumplimiento: crea un rol de IAM para gestionar los incidentes con AWS. **`policyUsageType`** (opcional) • Especifica si espera que la política se adjunte a un usuario, grupo o rol. • Tipo: cadena • Valores válidos: `IAM_USER` | `IAM_GROUP` | `IAM_ROLE` | `ANY` • Valor predeterminado: `ANY` • Requisito de cumplimiento: adjunte la política de confianza al rol de IAM creado
IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS	No aplicable
IAM_ROOT_ACCESS_KEY_CHECK	No aplicable
IAM_USER_NO_POLICIES_CHECK	No aplicable

Norma de AWS Config obligatoria	Parámetros necesarios
IAM_USER_UNUSED_CREDENTIALS_CHECK	**`maxCredentialUsageAge`** • El número máximo de días durante los que no se puede usar una credencial. • Tipo: Int • Predeterminado: 90 días • Requisito de cumplimiento: 90 días o más
INCOMING_SSH_DISABLED	No aplicable
MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	No aplicable
MULTI_REGION_CLOUD_TRAIL_ENABLED	No aplicable

Norma de AWS Config obligatoria	Parámetros necesarios
RESTRICTED_INCOMING_TRAFFIC	**`blockedPort1`** (opcional) • El número de puerto TCP bloqueado. • Tipo: int • Valor predeterminado: 20 • Requisito de cumplimiento: asegúrese de que ningún grupo de seguridad permita la entrada en los puertos bloqueados **`blockedPort2`** (opcional) • El número de puerto TCP bloqueado. • Tipo: int • Predeterminado: 21 • Requisito de cumplimiento: asegúrese de que ningún grupo de seguridad permita la entrada en los puertos bloqueados **`blockedPort3`** (opcional) • El número de puerto TCP bloqueado. • Tipo: int • Valor predeterminado: 3389 • Requisito de cumplimiento: asegúrese de que ningún grupo de seguridad permita la entrada en los puertos bloqueados **`blockedPort4`** (opcional) • El número de puerto TCP bloqueado. • Tipo: int • Predeterminado: 3306 • Requisito de cumplimiento: asegúrese de que ningún grupo de seguridad permita la entrada en los puertos bloqueados

Norma de AWS Config obligatoria	Parámetros necesarios
	`blockedPort5` (opcional) • El número de puerto TCP bloqueado. • Tipo: int • Predeterminado: 4333 • Requisito de cumplimiento: asegúrese de que ningún grupo de seguridad permita la entrada en los puertos bloqueados
ROOT_ACCOUNT_HARDWARE_MFA_ENABLED	No aplicable
ROOT_ACCOUNT_MFA_ENABLED	No aplicable
S3_BUCKET_LOGGING_ENABLED	**`targetBucket`** (opcional) • El bucket de S3 de destino para almacenar registros de acceso al servidor. • Tipo: cadena • Requisito de conformidad: habilitar el registro **`targetPrefix`** (opcional) • El prefijo del bucket de S3 para almacenar registros de acceso al servidor. • Tipo: cadena • Requisito de conformidad: identificar el bucket de S3 para el registro de CloudTrail
S3_BUCKET_PUBLIC_READ_PROHIBITED	No aplicable
VPC_DEFAULT_SECURITY_GROUP_CLOSED	No aplicable

Norma de AWS Config obligatoria	Parámetros necesarios
VPC_FLOW_LOGS_ENABLED	**`trafficType`** (opcional) • El `trafficType` de los registros de flujo. • Tipo: cadena • Requisito de cumplimiento: el registro de flujos está habilitado

Más recursos para CIS

- El Foundations Benchmark v1.2.0 CIS AWS
- Publicaciones del blog sobre Foundations Benchmark CIS AWS en el blog de seguridad de AWS.

CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0

AWS Audit Manager proporciona dos marcos prediseñados que admiten Foundations Benchmark v1.3 CIS AWS:

- CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0, nivel 1
- CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0, nivel 1 y 2

> **Note**
>
> Para obtener información sobre Foundations Benchmark v1.2.0 CIS AWS y los marcos de AWS Audit Manager que admiten esta versión del punto de referencia, consulte CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0.

Temas

¿Qué es CIS?

El CIS desarrolló el Foundations Benchmark CIS AWS v1.3.0, un conjunto de prácticas recomendadas de configuración de seguridad para AWS. Estas prácticas recomendadas aceptadas por la industria van más allá de las directrices de seguridad de alto nivel ya disponibles, ya que proporcionan a los usuarios de AWS procedimientos de implementación y evaluación claros y detallados.

Para obtener más información, consulte las publicaciones del blog CIS AWS Foundations Benchmark en el blog de seguridad de AWS.

Foundations Benchmark v1.3.0 CIS AWS proporciona una guía para configurar las opciones de seguridad para un subconjunto de Servicios de AWS, haciendo hincapié en las configuraciones fundamentales, comprobables e independientes de la arquitectura. Algunos de los Amazon Web Services específicos que se incluyen en este documento incluyen los siguientes:

- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (predeterminado)

Diferencia entre los CIS Benchmarks y los controles CIS

Los CIS Benchmarks son pautas de prácticas de seguridad específicas recomendadas para los productos de los proveedores. Desde sistemas operativos hasta servicios en la nube y dispositivos de red, los ajustes que se aplican a partir de un punto de referencia protegen los sistemas que utiliza su organización. Los controles CIS son pautas fundamentales de prácticas recomendadas que debe seguir su organización para protegerse de los vectores de ciberataques conocidos.

Ejemplos

- Los CIS Benchmarks son prescriptivos. Por lo general, hacen referencia a una configuración específica que se puede revisar y establecer en el producto del proveedor.

Ejemplo: CIS Amazon Web Services Foundations Benchmark v1.3.0 - 1.5 Asegúrese de que el MFA esté habilitado para la cuenta del “usuario raíz”.

Esta recomendación proporciona una guía prescriptiva sobre cómo comprobarlo y cómo configurarlo en la cuenta raíz para el entorno AWS.

- Los controles CIS son para su organización en su conjunto y no son específicos de un solo producto de un proveedor.

  Ejemplo: controles CIS v7.1 - Sub-Control 4.5 Utilice la autenticación multifactor para todos los accesos administrativos

  Este control describe lo que se espera que se aplique en su organización, pero no cómo debe aplicarlo a los sistemas y las cargas de trabajo que ejecuta (independientemente de dónde se encuentren).

Utilice estos marcos para respaldar la preparación de la auditoría

Puede utilizar los marcos Foundations Benchmark v1.3 CIS AWS en AWS Audit Manager para prepararse para las auditorías de CIS. También puede personalizar estos marcos y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza los marcos como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace basándose en los controles que se definen en el marco de CIS. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0, nivel 1	33	5	6	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS Config • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0, nivel 1 y 2	49	6	6	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

Para revisar una lista de las normas de AWS Config que se utilizan como mapeos de origen de datos para estos marcos estándar, descargue los siguientes archivos:

- AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0-Level-1.zip

- AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0,Level1-and-2.zip

Los controles de estos marcos no pretenden verificar si sus sistemas cumplen con el estándar CIS. Además, no pueden garantizarle que vaya a superar una auditoría de CIS. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar estos marcos en la pestaña Standard frameworks (Marcos estándar) de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de estos marcos, consulte Creación de las evaluaciones.

Cuando utiliza la consola Audit Manager para crear una evaluación a partir de estos marcos estándar, la lista de Servicios de AWS dentro del alcance se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos de los CIS Benchmarks. Si necesita editar la lista de servicios incluidos en estos marcos, puede hacerlo mediante las operaciones de la API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar estos marcos para que se adapten a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos para CIS

- Publicaciones del blog sobre Foundations Benchmark CIS AWS en el blog de seguridad de AWS.

CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0

AWS Audit Manager proporciona dos marcos estándar prediseñados compatibles con el AWS Foundations Benchmark v1.4.0 del Centro para la Seguridad en Internet (CIS):

- CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0, nivel 1

- CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0, nivel 1 y 2

> **Note**
>
> - Para obtener información sobre los marcos de Audit Manager compatibles con v1.2.0, consulte CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.2.0.
> - Para obtener información sobre los marcos de Audit Manager compatibles con la versión 1.3.0, consulte CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.3.0.

Temas

¿Qué son los CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0?

Los CIS Benchmarks para CIS Amazon Web Services Foundations Benchmark, v1.4.0, niveles 1 y 2, proporcionan una guía prescriptiva para configurar las opciones de seguridad para un subconjunto de Amazon Web Services. Hace hincapié en las configuraciones fundamentales, comprobables e independientes de la arquitectura. Algunos de los Amazon Web Services específicos que se incluyen en este documento incluyen los siguientes:

- AWS Identity and Access Management (IAM)
- Analizador de acceso de IAM
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS)

- Amazon Virtual Private Cloud

Diferencia entre los CIS Benchmarks y los controles CIS

Los CIS Benchmarks son pautas de prácticas de seguridad específicas recomendadas para los productos de los proveedores. Desde sistemas operativos hasta servicios en la nube y dispositivos de red, los ajustes que se aplican desde un punto de referencia protegen los sistemas que se utilizan. Los controles CIS son pautas fundamentales de prácticas recomendadas que debe seguir su organización para protegerse de los vectores de ciberataques conocidos.

Ejemplos

- Los CIS Benchmarks son prescriptivos. Por lo general, hacen referencia a una configuración específica que se puede revisar y establecer en el producto del proveedor.

  Ejemplo: CIS Amazon Web Services Foundations Benchmark v1.4.0 - 1.5 Asegúrese de que el MFA esté habilitado para la cuenta del “usuario raíz”.

  Esta recomendación proporciona una guía prescriptiva sobre cómo comprobarlo y cómo configurarlo en la cuenta raíz para el entorno AWS.
- Los controles CIS son para su organización en su conjunto y no son específicos de un solo producto de un proveedor.

  Ejemplo: controles CIS v7.1 - Sub-Control 4.5 Utilice la autenticación multifactor para todos los accesos administrativos

  Este control describe lo que se espera que se aplique en su organización. Sin embargo, no describe cómo aplicarlo a los sistemas y cargas de trabajo que se están ejecutando, independientemente de dónde se encuentren.

Utilice estos marcos para respaldar la preparación de la auditoría

Puede utilizar los marcos Foundations Benchmark v1.4.0 CIS AWSen AWS Audit Manager para prepararse para las auditorías de CIS. También puede personalizar estos marcos y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza los marcos como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace basándose en los controles que se definen en el

marco de CIS. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0, nivel 1	32	6	7	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management
CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0, nivel 1 y 2	50	8	7	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para revisar una lista de las normas de AWS Config que se utilizan como mapeos de origen de datos para estos marcos estándar, descargue los siguientes archivos:
>
> - AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.4.0-Level-1.zip
> - AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.4.0-Level-1-and-2.zip

Los controles de estos marcos no pretenden verificar si sus sistemas cumplen con el estándar de CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4.0. Además, no pueden garantizarle que vaya a superar una auditoría de CIS. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar estos marcos en la pestaña Standard frameworks (Marcos estándar) de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de estos marcos, consulte Creación de las evaluaciones.

Cuando utiliza la consola Audit Manager para crear una evaluación a partir de estos marcos estándar, la lista de Servicios de AWS dentro del alcance se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos de los CIS Benchmarks. Si necesita editar la lista de servicios incluidos en estos marcos, puede hacerlo mediante las operaciones de la API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar estos marcos para que se adapten a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos para CIS

- CIS Benchmarks del Centro para la seguridad de Internet (CIS)
- Publicaciones del blog sobre Foundations Benchmark CIS AWS en el blog de seguridad de AWS.

Grupo de implementación 1 de controles CIS v7.1

AWS Audit Manager proporciona un marco prediseñado que admite el grupo de implementación 1 de los controles CIS v7.1.

> **Note**
>
> Para obtener información sobre los controles CIS v8 IG1 y el marco de AWS Audit Manager que admite este estándar, consulte Grupo de implementación 1 de controles CIS v8.

AWS Audit Manager proporciona un marco prediseñado que sirve de apoyo al CIS para ayudarle a preparar la auditoría.

Temas

- ¿Qué son los controles CIS?
- Utilice este marco para respaldar la preparación de la auditoría
- Más recursos para CIS

¿Qué son los controles CIS?

Los controles CIS son un conjunto de acciones priorizadas que, en conjunto, forman un conjunto de prácticas recomendadas de defensa en profundidad. Estas prácticas recomendadas mitigan los ataques más comunes contra sistemas y redes. El Grupo de Implementación 1 se define generalmente para una organización con recursos limitados y experiencia en ciberseguridad que está disponible para implementar subcontroles.

Diferencia entre los controles CIS y los CIS Benchmarks

Los controles CIS son pautas fundamentales de prácticas recomendadas que una organización puede seguir para protegerse de los vectores de ciberataques conocidos. Los CIS Benchmarks son pautas de prácticas de seguridad específicas recomendadas para los productos de los proveedores. Desde sistemas operativos hasta servicios en la nube y dispositivos de red, los ajustes que se aplican desde un punto de vista comparativo protegen los sistemas que se utilizan.

Ejemplos

- Los CIS Benchmarks son prescriptivos. Por lo general, hacen referencia a una configuración específica que se puede revisar y establecer en el producto del proveedor.

  - Ejemplo: CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Asegúrese de que el MFA esté habilitado para la cuenta del “usuario raíz”.
  - Esta recomendación proporciona una guía prescriptiva sobre cómo comprobarlo y cómo configurarlo en la cuenta raíz para el entorno AWS.
- Los controles CIS son para su organización en su conjunto y no son específicos de un solo producto de un proveedor.
  - Ejemplo: controles CIS v7.1 - Sub-Control 4.5 Utilice la autenticación multifactor para todos los accesos administrativos
  - Este control describe lo que se espera que se aplique en su organización. Sin embargo, no le indica cómo debe aplicarlo a los sistemas y las cargas de trabajo que está ejecutando (independientemente de dónde se encuentren).

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco controles CIS v7.1 IG1 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de CIS. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace basándose en los controles que se definen en el marco controles CIS v7.1 IG1. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco controles CIS v7.1 IG1 son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
Controles CIS v7.1 IG1	21	22	16	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Managemen t

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_CIS-Controls-v7.1-IG1.zip .

Los controles de este marco no tienen por objeto comprobar si sus sistemas cumplen con los controles CIS. Además, no pueden garantizarle que vaya a superar una auditoría de CIS. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos de los controles CIS. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones

de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos para CIS

- Controles CIS v7.1 IG1

Grupo de implementación 1 de controles CIS v8

AWS Audit Manager proporciona un marco estándar prediseñado compatible con el grupo de implementación 1 de los controles CIS v8.

> **Note**
>
> Para obtener información sobre controles CIS v7.1 IG1 y el marco de AWS Audit Manager que admite este estándar, consulte Grupo de implementación 1 de controles CIS v7.1.

Temas

¿Qué son los controles CIS?

Los controles de seguridad críticos de CIS (controles CIS) son un conjunto de salvaguardas priorizado para mitigar los ciberataques más frecuentes contra sistemas y redes. Están mapeados y referenciados por múltiples marcos legales, regulatorios y políticos. La versión 8 de los controles CIS se ha mejorado para adaptarse a los sistemas y software modernos. La transición a la informática basada en la nube, la virtualización, la movilidad, la subcontratación, el trabajo desde casa y los cambios en las tácticas de los atacantes impulsaron la actualización. Esta actualización contribuye a la seguridad de las empresas a medida que se trasladan a entornos totalmente en la nube o híbridos.

Diferencia entre los controles CIS y los CIS Benchmarks

Los controles CIS son pautas fundamentales de prácticas recomendadas que una organización puede seguir para protegerse de los vectores de ciberataques conocidos. Los CIS Benchmarks son pautas de prácticas de seguridad específicas recomendadas para los productos de los proveedores. Desde sistemas operativos hasta servicios en la nube y dispositivos de red, los ajustes que se aplican desde un punto de vista comparativo protegen los sistemas que se utilizan.

Ejemplos

- Los CIS Benchmarks son prescriptivos. Por lo general, hacen referencia a una configuración específica que se puede revisar y establecer en el producto del proveedor.
  - Ejemplo: CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Asegúrese de que el MFA esté habilitado para la cuenta del “usuario raíz”.
  - Esta recomendación proporciona una guía prescriptiva sobre cómo comprobarlo y cómo configurarlo en la cuenta raíz para el entorno AWS.
- Los controles CIS son para su organización en su conjunto y no son específicos de un solo producto de un proveedor.
  - Ejemplo: controles CIS v7.1 - Sub-Control 4.5 Utilice la autenticación multifactor para todos los accesos administrativos
  - Este control describe lo que se espera que se aplique en su organización. Sin embargo, no le indica cómo debe aplicarlo a los sistemas y las cargas de trabajo que está ejecutando (independientemente de dónde se encuentren).

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco controles CIS v8 IG1 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de CIS. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace basándose en los controles que se definen en el marco controles CIS v8. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas

y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco controles CIS v8 son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
Controles CIS v8 IG1	25	31	15	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management • AWS License Manager

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_CIS-Controls-v8-IG1.zip.

Los controles de este marco no tienen por objeto comprobar si sus sistemas cumplen con los controles CIS. Además, no pueden garantizarle que vaya a superar una auditoría de CIS. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos de los controles CIS. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos para CIS

- Controles CIS v8

Referencia moderada de FedRAMP

AWS Audit Manager proporciona un marco de referencia moderado de FedRAMP para ayudarlo en la preparación de la auditoría.

Temas

- ¿Qué es FedRAMP?
- Utilice este marco para respaldar la preparación de la auditoría
- Más recursos de FedRAMP

¿Qué es FedRAMP?

El Programa Federal de Administración de Riesgos y Autorizaciones (FedRAMP) se estableció en 2011. Proporciona un enfoque rentable y basado en el riesgo para la adopción y el uso de los servicios en la nube por parte del gobierno federal de EE. UU. FedRAMP permite a las agencias federales utilizar tecnologías de nube modernas, con énfasis en la seguridad y la protección de la información federal.

Para obtener más información sobre los controles de referencia moderados de FedRAMP, consulte la plantilla de procedimientos de casos de pruebas de seguridad moderada de FedRAMP.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco de referencia moderado de FedRAMP como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de FedRAMP. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el marco. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco de referencia moderada de FedRAMP son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
Referencia moderada de FedRAMP	303	908	325	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_FedRAMP-Moderate-Baseline.zip.

Los controles de este marco no tienen por objeto comprobar si los sistemas cumplen con FedRAMP. Además, no pueden garantizarle que vaya a superar una auditoría del FedRAMP. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos de la referencia moderada de FedRAMP. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos de FedRAMP

- AWS Página de conformidad para FedRAMP
- AWS Publicaciones del blog de FedRAMP

Reglamento General de Protección de Datos (RGPD)

AWS Audit Manager proporciona un marco estándar prediseñado que respalda el RGPD. De forma predeterminada, este marco contiene solo controles manuales. Estos controles manuales no recopilan pruebas automáticamente. Sin embargo, si quiere automatizar la recopilación de pruebas para algunos controles contemplados en el RGPD, puede utilizar la característica de control personalizado que se incluye en AWS Audit Manager. Para obtener más información, consulte Utilice este marco para respaldar la preparación de la auditoría.

Temas

¿Qué es el RGPD?

El RGPD es una nueva ley europea de privacidad que entró en vigor el 25 de mayo de 2018. El RGPD sustituye a la Directiva de protección de datos de la UE, también conocida como Directiva 95/46/EC. Su objetivo es armonizar las leyes de protección de datos en toda la Unión Europea (UE). Para ello, aplica una única ley de protección de datos que es vinculante en todos los estados miembros de la UE.

El RGPD se aplica a todas las organizaciones establecidas en la UE y a las organizaciones (independientemente de si están establecidas en la UE) que procesan los datos personales de los interesados de la UE en relación con la oferta de bienes o servicios a interesados en la UE o con el seguimiento del comportamiento que tiene lugar dentro de la UE. Los datos personales son cualquier información relacionada con una persona física identificada o identificable.

Puede encontrar el marco del RGPD en la página de la biblioteca de marcos de AWS Audit Manager. Para obtener más información, consulte el Centro del RGPD.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco del RGPD en AWS Audit Manager como ayuda para prepararse para las auditorías.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
RGPD	0	371	10	Ninguna

Puede encontrar el marco del RGPD en la pestaña Marcos estándar del Biblioteca de marcos en Audit Manager. Dado que este marco estándar solo contiene controles manuales, ningún Servicios de AWS está incluido en su ámbito de aplicación.

> **Note**
>
> Si desea automatizar la recopilación de pruebas para el RGPD, puede usar Audit Manager para crear sus propios controles personalizados para el RGPD. La siguiente tabla proporciona recomendaciones sobre el origen de datos de AWS que puede asignar a los requisitos del RGPD en sus controles personalizados. Aunque algunas de las siguientes origen de datos están asignadas a varios controles, tenga en cuenta que solo se le cobrará una vez por cada evaluación de recursos.
> En las siguientes recomendaciones se utilizan AWS Config y AWS Security Hub como origen de datos. Para obtener pruebas de este origen de datos, asegúrese de hacer lo siguiente:
>
> - Confirme que ha seguido las instrucciones para activar y configurar AWS Config y AWS Security Hub en tu Cuenta de AWS.
> - Confirme que ha incluido AWS Config y Security Hub como servicios incluidos en el ámbito de aplicación. Para revisar la lista de servicios incluidos en el ámbito de su evaluación, consulte Revisar una evaluación, en la pestaña Servicios de AWS. Para editar esta lista, consulte Editar Servicios de AWS dentro del alcance.
>
> Una vez configurados ambos servicios de esta manera, Audit Manager recopila pruebas cada vez que se realiza una evaluación para la norma AWS Config especificada o el control de Security Hub.

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
Artículo 25 Protección de datos desde el	Capítulo 4: Controlador y procesador	Puede crear un control personalizado en AWS Audit Manager que respalde este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas:

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
diseño y por defecto.1		• Mostrar todos los eventos de la cuenta raíz a lo largo del período • el bucket AWS CloudTrail no es público • Muestre todas las políticas con una `Allow:*:*` y enumere todos los principales y servicios que utilizan esas políticas Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config como el tipo de origen de datos y seleccione las siguientes normas administradas de AWS Config como mapeos de origen de datos: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Elija AWS Security Hub como tipo de origen de datos y seleccione los siguientes controles de Security Hub como asignaciones de origen de datos: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6)

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
		• 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
Artículo 25 Protección de datos desde el diseño y por defecto.2	Capítulo 4: Controlador y procesador	Puede crear un control personalizado en AWS Audit Manager que respalde este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Mostrar todos los eventos de la cuenta raíz a lo largo del período • el bucket AWS CloudTrail no es público • Muestre todas las políticas con una `Allow:*:*` y enumere todos los principales y servicios que utilizan esas políticas Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config como el tipo de origen de datos y seleccione las siguientes normas administradas de AWS Config como mapeos de origen de datos: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Elija AWS Security Hub como tipo de origen de datos y seleccione los siguientes controles de Security Hub como asignaciones de origen de datos: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16)

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
		• 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11)

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
		• 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
Artículo 25 Protección de datos desde el diseño y por defecto.3	Capítulo 4: Controlador y procesador	Puede crear un control personalizado en AWS Audit Manager que respalde este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Mostrar todos los eventos de la cuenta raíz a lo largo del período • el bucket AWS CloudTrail no es público • Muestre todas las políticas con una `Allow:*:*` y enumere todos los principales y servicios que utilizan esas políticas Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config como el tipo de origen de datos y seleccione las siguientes normas administradas de AWS Config como mapeos de origen de datos: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Elija AWS Security Hub como tipo de origen de datos y seleccione los siguientes controles de Security Hub como asignaciones de origen de datos: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16)

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
		• 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11)

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
		• 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
Artículo 30 Registros de las actividades de procesamiento.1	Capítulo 4: Controlador y procesador	Puede crear un control personalizado en AWS Audit Manager que respalde este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Mostrar todos los eventos de la cuenta raíz a lo largo del período Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config como el tipo de origen de datos y seleccione las siguientes normas administradas de AWS Config como mapeos de origen de datos: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUDTRAIL_SECURITY_TRAIL_ENABLED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Elija AWS Security Hub como el tipo de origen de datos y seleccione el siguiente control de Security Hub como mapeo del origen de datos: • Config.1

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
Artículo 30 Registros de las actividades de procesamiento.2	Capítulo 4: Controlador y procesador	Puede crear un control personalizado en AWS Audit Manager que respalde este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Mostrar todos los eventos de la cuenta raíz a lo largo del período Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config como el tipo de origen de datos y seleccione las siguientes normas administradas de AWS Config como mapeos de origen de datos: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Elija AWS Security Hub como el tipo de origen de datos y seleccione el siguiente control de Security Hub como mapeo del origen de datos: • Config.1

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
Artículo 30 Registros de las actividades de procesamiento.3	Capítulo 4: Controlador y procesador	Puede crear un control personalizado en AWS Audit Manager que respalde este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Mostrar todos los eventos de la cuenta raíz a lo largo del período • el bucket AWS CloudTrail no es público • Muestre todas las políticas con una `Allow:*:*` y enumere todos los principales y servicios que utilizan esas políticas Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config como el tipo de origen de datos y seleccione las siguientes normas administradas de AWS Config como mapeos de origen de datos: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Elija AWS Security Hub como el tipo de origen de datos y seleccione el siguiente control de Security Hub como mapeo del origen de datos: • Config.1

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
Artículo 30 Registros de las actividades de procesamiento.4	Capítulo 4: Controlador y procesador	Puede crear un control personalizado en AWS Audit Manager que respalde este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Mostrar todos los eventos de la cuenta raíz a lo largo del período • el bucket AWS CloudTrail no es público • Muestre todas las políticas con una `Allow:*:*` y enumere todos los principales y servicios que utilizan esas políticas Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config como el tipo de origen de datos y seleccione las siguientes normas administradas de AWS Config como mapeos de origen de datos: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Elija AWS Security Hub como el tipo de origen de datos y seleccione el siguiente control de Security Hub como mapeo del origen de datos: • Config.1

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
Artículo 30 Registros de las actividades de procesamiento.5	Capítulo 4: Controlador y procesador	Puede crear un control personalizado en AWS Audit Manager que respalde este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Mostrar todos los eventos de la cuenta raíz a lo largo del período Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config como el tipo de origen de datos y seleccione las siguientes normas administradas de AWS Config como mapeos de origen de datos: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Elija AWS Security Hub como el tipo de origen de datos y seleccione el siguiente control de Security Hub como mapeo del origen de datos: • Config.1

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
Artículo 32 Seguridad del procesamiento.1	Capítulo 4: Controlador y procesador	Puede crear un control personalizado en AWS Audit Manager que respalde este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Muestra el cifrado de los datos en reposo para todos los servicios • Muestra el cifrado de los datos en tránsito para todos los servicios • MFA Delete habilitada para Amazon S3 • Todos los escaneos de Amazon Inspector • Mostrar todas las instancias que no están habilitadas para Amazon Inspector • Mostrar todos los equilibradores de carga que escuchan en HTTPS (SSL) • Encriptado en reposo AWS CloudTrail • Alertas de Amazon CloudWatch para AWS Config que muestran todos los cambios y todos los ajustes comentados • Toda la actividad raíz Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config como el tipo de origen de datos y seleccione las siguientes normas administradas de AWS Config como mapeos de origen de datos: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
		• ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
		• ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
Artículo 32 Seguridad del procesamiento.2	Capítulo 4: Controlador y procesador	Puede crear un control personalizado en AWS Audit Manager que respalde este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Muestra el cifrado de los datos en reposo para todos los servicios • Muestra el cifrado de los datos en tránsito para todos los servicios • MFA Delete habilitada para Amazon S3 • Todos los escaneos de Amazon Inspector • Mostrar todas las instancias que no están habilitadas para Amazon Inspector • Mostrar todos los equilibradores de carga que escuchan en HTTPS (SSL) • Encriptado en reposo AWS CloudTrail • Alertas de Amazon CloudWatch para AWS Config que muestran todos los cambios y todos los ajustes comentados • Toda la actividad raíz Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config como el tipo de origen de datos y seleccione las siguientes normas administradas de AWS Config como mapeos de origen de datos: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
		• ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
		• ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
Artículo 32 Seguridad del procesamiento.3	Capítulo 4: Controlador y procesador	Puede crear un control personalizado en AWS Audit Manager que respalde este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Muestra el cifrado de los datos en reposo para todos los servicios • Muestra el cifrado de los datos en tránsito para todos los servicios • MFA Delete habilitada para Amazon S3 • Todos los escaneos de Amazon Inspector • Mostrar todas las instancias que no están habilitadas para Amazon Inspector • Mostrar todos los equilibradores de carga que escuchan en HTTPS (SSL) • Encriptado en reposo AWS CloudTrail • Alertas de Amazon CloudWatch para AWS Config que muestran todos los cambios y todos los ajustes comentados • Toda la actividad raíz Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config como el tipo de origen de datos y seleccione las siguientes normas administradas de AWS Config como mapeos de origen de datos: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
		• ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
		• ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
Artículo 32 Seguridad del procesamiento.4	Capítulo 4: Controlador y procesador	Puede crear un control personalizado en AWS Audit Manager que respalde este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Muestra el cifrado de los datos en reposo para todos los servicios • Muestra el cifrado de los datos en tránsito para todos los servicios • MFA Delete habilitada para Amazon S3 • Todos los escaneos de Amazon Inspector • Mostrar todas las instancias que no están habilitadas para Amazon Inspector • Mostrar todos los equilibradores de carga que escuchan en HTTPS (SSL) • Encriptado en reposo AWS CloudTrail • Alertas de Amazon CloudWatch para AWS Config que muestran todos los cambios y todos los ajustes comentados • Toda la actividad raíz Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config como el tipo de origen de datos y seleccione las siguientes normas administradas de AWS Config como mapeos de origen de datos: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
		• ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Nombre del control	Conjunto de control	Mapeo de origen de datos de control recomendado
		• ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

Después de crear los nuevos controles personalizados, puede agregarlos a un marco de RGPD personalizado. Para más información, consulte Crear un marco personalizado y Editar un marco personalizado. A continuación, puede crear una evaluación a partir del marco personalizado del RGPD. De esta forma, AWS Audit Manager puede recopilar pruebas automáticamente para los controles personalizados que haya agregado. Para obtener instrucciones sobre cómo crear una evaluación a partir de un marco, consulte Creación de las evaluaciones.

Más recursos para RGPD

- Centro del RGPD
- AWS Publicaciones de blog sobre RGPD

Ley Gramm-Leach-Bliley

AWS Audit Manager proporciona un marco prediseñado que respalda la Ley Gramm-Leach-Bliley (GLBA).

Temas

- ¿Qué es la Ley Gramm-Leach-Bliley (GLBA)?
- Utilice este marco para respaldar la preparación de la auditoría

¿Qué es la Ley Gramm-Leach-Bliley (GLBA)?

La Ley Gramm-Leach-Bliley (Ley GLB o GLBA), también conocida como Ley de Modernización de los Servicios Financieros de 1999, es una ley federal promulgada en los Estados Unidos para controlar la forma en que las instituciones financieras manejan la información privada de las personas. La Ley consta de tres secciones. La primera es la Norma de Privacidad Financiera, que regula la recopilación y divulgación de información financiera privada. La segunda es la Norma

de Salvaguardas, que estipula que las instituciones financieras deben implementar programas de seguridad para proteger dicha información. La tercera son las disposiciones sobre el uso de pretextos, que prohíben la práctica del uso de pretextos (acceder a información privada con falsos pretextos). La ley también exige que las instituciones financieras entreguen a los clientes avisos de privacidad por escrito que expliquen sus prácticas de intercambio de información.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco de la Ley Gramm-Leach-Bliley (GLBA) como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de la GLBA. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco de la GLBA como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para una auditoría de la GLBA. En su evaluación, puede especificar las Cuentas de AWS y los servicios que desea incluir en el ámbito de su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el marco de la GLBA. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco GLBA son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
GLBA	4	110	16	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
				• AWS Security Hub

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_GLBA.zip.

Los controles de este marco de AWS Audit Manager no tienen por objeto verificar si sus sistemas cumplen con la norma de la GLBA. Además, no pueden garantizarle que vaya a superar una auditoría del GLBA. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar el marco de la GLBA en la pestaña Marcos estándar del Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos de la GLBA. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

GxP 21 CFR Parte 11

AWS Audit Manager proporciona un marco prediseñado que respalda la normativa GxP CFR, Parte 11, basada en las prácticas recomendadas de AWS.

> **Note**
>
> Para obtener información sobre el GxP EU Anexo 11 y el marco de Audit Manager que lo respalda, consulte GxP UE Anexo 11.

Temas

¿Qué es GxP CFR Parte 11?

GxP se refiere a las normas y directrices aplicables a las organizaciones de ciencias de la vida que fabrican alimentos y productos médicos. Entre los productos médicos incluidos en esta categoría se incluyen los medicamentos, los dispositivos médicos y las aplicaciones de software médico. El objetivo general de los requisitos de GxP es garantizar que los alimentos y los productos médicos sean seguros para los consumidores. También es para garantizar la integridad de los datos que se utilizan para tomar decisiones de seguridad relacionadas con los productos.

El término GxP abarca una amplia gama de actividades relacionadas con el cumplimiento. Estas incluyen las buenas prácticas de laboratorio (Good Laboratory Practices, GLP), las buenas prácticas clínicas (Good Clinical Practices, GCP) y las buenas prácticas de fabricación (Good Manufacturing Practices, GMP). Cada uno de estos diferentes tipos de actividades implica requisitos específicos del producto que las organizaciones de ciencias de la vida deben implementar. Esto se basa en el tipo de productos que fabrican las organizaciones, así como en el país en el que se venden sus productos. Cuando las organizaciones de ciencias de la vida utilizan sistemas computarizados para realizar determinadas actividades de GxP, deben asegurarse de que el sistema GxP computarizado se desarrolle, valide y funcione de manera adecuada para el uso previsto del sistema.

Para obtener un enfoque integral del uso de la nube de AWS para los sistemas GxP, consulte el documento técnico Consideraciones sobre el uso de productos AWS en los sistemas GxP.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco GxP 21 CFR Parte 11 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de GxP. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el marco GxP 21 CFR Parte 11. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco GxP CFR, Parte 11, son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
GxP 21 CFR Parte 11	13	14	7	• AWS CloudTrail • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_GxP-21-CFR-Part-11.zip.

Los controles en este marco de AWS Audit Manager no tienen por objeto comprobar si los sistemas cumplen con la normativa GxP. Además, no pueden garantizarle que vaya a superar una auditoría del GxP. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco GxP CFR Parte 11. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos para GxP

- AWS Página de cumplimiento para GxP
- Consideraciones sobre el uso de productos de AWS en sistemas GxP

GxP UE Anexo 11

AWS Audit Manager proporciona un marco prediseñado que respalda las normas de GxP UE Anexo 11 basadas en las prácticas recomendadas de AWS.

> **Note**
>
> Para obtener información sobre GxP 21 CFR Parte 11 y el marco de Audit Manager que lo respalda, consulte GxP 21 CFR Parte 11.

Temas

¿Qué es GxP UE Anexo 11?

El marco GxP UE Anexo 11 es el equivalente europeo del marco FDA 21 CFR Parte 11 en los Estados Unidos. Este anexo se aplica a todos los tipos de sistemas computarizados que se utilizan como parte de las actividades reguladas por las buenas prácticas de fabricación (GMP). Un sistema computarizado es un conjunto de componentes de software y hardware que, en conjunto, cumplen ciertas funcionalidades. La aplicación debe estar validada y la infraestructura de TI debe estar calificada. Cuando un sistema computarizado sustituya a una operación manual, no debería producirse una disminución en la calidad del producto, el control del proceso o la garantía de calidad. No debe haber ningún aumento en el riesgo general del proceso.

El anexo 11 forma parte de las directrices europeas sobre buenas prácticas de fabricación y define los términos de referencia de los sistemas computarizados que utilizan las organizaciones de la industria farmacéutica. El anexo 11 funciona como una lista de verificación que permite a las agencias reguladoras europeas establecer los requisitos para los sistemas computarizados relacionados con los productos farmacéuticos y los dispositivos médicos. Las directrices establecidas por la Comisión de los Comités Europeos no están muy alejadas de las de la FDA (21 CFR, parte 11). En el anexo 11 se definen los criterios por los que se considera que se gestionan los registros electrónicos y las firmas electrónicas.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco GxP UE Anexo 11 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de GxP. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el marco del GxP UE Anexo 11. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco GxP UE Anexo 11 son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
GxP UE Anexo 11	19	13	3	• Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_GxP-EU-Annex-11.zip.

Los controles de este marco no tienen por objeto verificar si sus sistemas cumplen con los requisitos del GxP UE Anexo 11. Además, no pueden garantizarle que vaya a superar una auditoría del GxP.

AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco GxP UE Anexo 11. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Ley de Portabilidad y Responsabilidad de Seguros Médicos de EE. UU (HIPAA) Norma de seguridad de 2003

AWS Audit Manager proporciona un marco prediseñado que respalda las normas de la HIPAA para ayudarlo en la preparación de la auditoría.

> **Note**
>
> Este marco se denominaba anteriormente HIPAA en la biblioteca de marcos. El 8 de marzo de 2023, actualizamos el nombre de este marco a Norma de Seguridad de la HIPAA de 2003 para diferenciarlo de la Norma general de seguridad definitiva de la HIPAA de 2013.
> Para obtener información sobre la Norma general de seguridad definitiva de la HIPAA de 2013 y el marco de Audit Manager que respalda este estándar, consulte Norma general de seguridad definitiva de la Ley de Portabilidad y Responsabilidad de Seguros Médicos (Health Insurance Portability and Accountability Act, HIPAA) de 2013.

Temas

¿Qué es la HIPAA y la Norma de Seguridad de la HIPAA de 2003?

La Ley estadounidense de Portabilidad y Responsabilidad de Seguros Médicos de 1996 (HIPAA) es una legislación que ayuda a los trabajadores estadounidenses a conservar la cobertura del seguro médico cuando cambian o pierden su empleo. La legislación también busca fomentar los registros médicos electrónicos para mejorar la eficacia y la calidad del sistema de salud de los EE. UU. mediante un mejor intercambio de información.

Además de aumentar el uso de los registros médicos electrónicos, la HIPAA incluye disposiciones para proteger la seguridad y la privacidad de la información de salud protegida (protected health information, PHI). La PHI incluye un conjunto muy amplio de datos de salud de identificación personal y relacionados con la salud. Esto incluye información sobre seguros y facturación, datos de diagnóstico, datos de atención clínica y resultados de laboratorio, como imágenes y resultados de pruebas.

El Departamento de Salud y Servicios Humanos de los Estados Unidos publicó una norma de seguridad definitiva en febrero de 2003. Esta regla establece estándares nacionales para proteger la confidencialidad, integridad y disponibilidad de la información médica electrónica protegida.

Las normas de la HIPAA se aplican a las entidades cubiertas. Estas incluyen hospitales, proveedores de servicios médicos, planes de salud patrocinados por el empleador, centros de investigación y compañías de seguros que tratan directamente con los pacientes y sus datos. El requisito de la HIPAA de proteger la PHI también se extiende a los socios comerciales.

Para obtener más información sobre cómo HIPAA e HITECH protegen la información de salud, consulte la página web Privacidad de la información de salud del Departamento de Salud y Servicios Humanos de los EE. UU.

Un número creciente de proveedores de atención médica, pagadores y profesionales de TI utilizan servicios en la nube basados en utilidades de AWS para procesar, almacenar y transmitir información sanitaria protegida (PHI). AWS permite a las entidades cubiertas y a sus asociados comerciales sujetos a la HIPAA utilizar el entorno seguro de AWS para procesar, mantener y almacenar información sanitaria protegida.

Para obtener instrucciones sobre cómo puede utilizar AWS para el procesamiento y almacenamiento de la información de salud, consulte el documento técnico Architecting for HIPAA Security and Compliance on Amazon Web Services.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco Norma de Seguridad de la HIPAA de 2003 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de la HIPAA. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el marco de la HIPAA. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco de la Norma de Seguridad de la HIPAA de 2003 son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
Norma de seguridad de la HIPAA de 2003	35	53	5	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
				• AWS Security Hub

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_HIPAA-Security-Rule-2003.zip.

Los controles de este marco de AWS Audit Manager no tienen por objeto verificar si sus sistemas cumplen con la norma HIPAA. Además, no pueden garantizar que vaya a superar una auditoría de la HIPAA. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco de la HIPAA. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos de la HIPAA

- Privacidad de la información de salud del Departamento de Salud y Servicios Humanos de los EE. UU.
- La norma de seguridad del Departamento de Salud y Servicios Humanos de los EE. UU.
- Arquitectura de seguridad de HIPAA y cumplimiento de servicios Amazon Web
- Página de cumplimiento de la HIPAA de AWS

Norma general de seguridad definitiva de la Ley de Portabilidad y Responsabilidad de Seguros Médicos (Health Insurance Portability and Accountability Act, HIPAA) de 2013

AWS Audit Manager proporciona un marco prediseñado que respalda las normas de la HIPAA para ayudarlo en la preparación de la auditoría.

> **Note**
>
> Para obtener información sobre la Norma de seguridad de la HIPAA de 2003 y el marco de AWS Audit Manager que respalda esta norma, consulte Ley de Portabilidad y Responsabilidad de Seguros Médicos de EE. UU (HIPAA) Norma de seguridad de 2003.

Temas

¿Qué es la HIPAA y la norma general de seguridad definitiva de la HIPAA?

La Ley estadounidense de Portabilidad y Responsabilidad de Seguros Médicos de 1996 (Health Insurance Portability and Accountability Act, HIPAA) es una legislación que ayuda a los trabajadores estadounidenses a conservar la cobertura del seguro médico cuando cambian o pierden su empleo. La legislación también busca fomentar los registros médicos electrónicos para mejorar la eficacia y la calidad del sistema de salud de los EE. UU. mediante un mejor intercambio de información.

Además de aumentar el uso de los registros médicos electrónicos, la HIPAA incluye disposiciones para proteger la seguridad y la privacidad de la información de salud protegida (protected health information, PHI). La PHI incluye un conjunto muy amplio de datos de salud de identificación personal y relacionados con la salud. Esto incluye información sobre seguros y facturación, datos de diagnóstico, datos de atención clínica y resultados de laboratorio, como imágenes y resultados de pruebas.

La norma general de seguridad definitiva de la HIPAA, que entró en vigor en 2013, implementa una serie de actualizaciones de todas las normas aprobadas anteriormente. Las modificaciones de las normas de seguridad, privacidad, notificación de infracciones y cumplimiento tenían por objeto mejorar la confidencialidad y la seguridad en el intercambio de datos.

Las normas de la HIPAA se aplican a las entidades cubiertas. Estas incluyen hospitales, proveedores de servicios médicos, planes de salud patrocinados por el empleador, centros de investigación y compañías de seguros que tratan directamente con los pacientes y sus datos. Como parte de las actualizaciones generales, muchas de las normas de la HIPAA que se aplican a las entidades cubiertas ahora también se aplican a los socios comerciales.

Para obtener más información sobre cómo HIPAA e HITECH protegen la información de salud, consulte la página web Privacidad de la información de salud del Departamento de Salud y Servicios Humanos de los EE. UU.

Un número creciente de proveedores de atención médica, pagadores y profesionales de TI utilizan servicios en la nube basados en utilidades de AWS para procesar, almacenar y transmitir información sanitaria protegida (PHI). AWS permite a las entidades cubiertas y a sus asociados comerciales sujetos a la HIPAA utilizar el entorno seguro de AWS para procesar, mantener y almacenar información sanitaria protegida. Para obtener instrucciones sobre cómo puede utilizar AWS para el procesamiento y almacenamiento de la información de salud, consulte el documento técnico Architecting for HIPAA Security and Compliance on Amazon Web Services.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco norma general de seguridad definitiva de la HIPAA de 2013 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de la HIPAA. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza

a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el marco de la HIPAA. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco de la norma general de seguridad definitiva de la HIPAA de 2013 son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
Norma general de seguridad definitiva de la HIPAA de 2013	39	46	5	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_HIPAA-Final-Omnibus-Security-Rule-2013.zip.

Los controles de este marco de AWS Audit Manager no tienen por objeto verificar si sus sistemas cumplen con la norma HIPAA. Además, no pueden garantizar que vaya a superar una auditoría de

la HIPAA. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco de la HIPAA. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos de la HIPAA

- Privacidad de la información de salud del Departamento de Salud y Servicios Humanos de los EE. UU.
- Elaboración de normas generales de la HIPAA del Departamento de Salud y Servicios Humanos de los EE. UU.
- Arquitectura de seguridad de HIPAA y cumplimiento de servicios Amazon Web
- Página de cumplimiento de la HIPAA de AWS

Anexo A de la norma de la ISO/IEC 27001:2013

AWS Audit Manager proporciona un marco estándar prediseñado que estructura y automatiza las evaluaciones del anexo A de la norma de la ISO/IEC 27001:2013.

Temas

- ¿Qué es el anexo A de la norma de la ISO/IEC 27001:2013?

¿Qué es el anexo A de la norma de la ISO/IEC 27001:2013?

La Comisión Electrotécnica Internacional (International Electrotechnical Commission, IEC) y la Organización Internacional de Normalización (International Organization for Standardization, ISO) son organizaciones independientes, no gubernamentales y sin fines de lucro que desarrollan y publican normas internacionales totalmente basadas en el consenso.

El anexo A de la norma de la ISO/IEC 27001:2013 es una norma de gestión de la seguridad que especifica las prácticas recomendadas de gestión de la seguridad y los controles de seguridad integrales que siguen la guía de mejores prácticas de la ISO/IEC 27002. Esta norma internacional especifica los requisitos sobre cómo establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información en su organización. Entre estos estándares, se incluyen los requisitos sobre la evaluación y el tratamiento de los riesgos de seguridad de la información, que se adaptan a las necesidades de su organización. Los requisitos de esta norma internacional son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco de AWS Audit Manager del anexo A de la norma de la ISO/IEC 27001:2013 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de control de acuerdo con los requisitos del anexo A de la norma de la ISO/IEC 27001:2013. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para una auditoría del anexo A de la norma de la ISO/IEC 27001:2013. En su evaluación, puede especificar las Cuentas de AWS y los servicios que desea incluir en el ámbito de su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el marco del anexo A de la norma de la ISO/IEC 27001:2013. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas

y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
Anexo A de la norma de la ISO-IEC 27001:2013	50	64	35	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_ISO-IEC-27001-2013-Annex-A.zip.

Los controles de este marco de AWS Audit Manager no tienen por objeto verificar si sus sistemas cumplen con este estándar internacional. Además, no pueden garantizarle que vaya a superar una auditoría de la ISO/IEC. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar el marco del anexo A de la norma de la ISO/IEC 27001:2013 en la pestaña Marcos estándar de Audit Manager. Biblioteca de marcos

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco del anexo A de la norma de la ISO-IEC 27001:2013. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones. Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos del anexo A de la norma de la ISO/IEC 27001:2013

- Para obtener más información sobre esta norma internacional, consulte la norma de la ISO/IEC 27001:2013 en la tienda web de ANSI.

NIST 800-53 (Rev. 5) Low-Moderate-High

AWS Audit Manager proporciona un marco prediseñado que estructura y automatiza las evaluaciones del estándar de cumplimiento del NIST 800-53, basándose en las prácticas recomendadas de AWS.

> **Note**
>
> - Para obtener información sobre el marco de Audit Manager compatible con NIST 800-171, consulte NIST SP 800-171 (Rev. 2).
> - Para obtener información sobre el marco de Audit Manager compatible con el marco de ciberseguridad del NIST, consulte Marco de Ciberseguridad del NIST versión 1.1.

Temas

- ¿Qué es NIST 800-53?
- Utilice este marco para respaldar la preparación de la auditoría

- Más recursos del NIST

¿Qué es NIST 800-53?

El Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST) se fundó en 1901 y ahora forma parte del Departamento de Comercio de los Estados Unidos. El NIST es uno de los laboratorios de ciencias físicas más antiguos de los Estados Unidos. El Congreso de los Estados Unidos creó la agencia para mejorar lo que en ese momento era una infraestructura de medición de segunda categoría. Las infraestructuras constituían un importante desafío para la competitividad industrial de Estados Unidos, que se había quedado rezagada con respecto a otras potencias económicas como el Reino Unido y Alemania.

Los controles de seguridad del NIST 800-53 se aplican generalmente a los sistemas de información federales de los EE. UU. Por lo general, se trata de sistemas que deben pasar por un proceso formal de evaluación y autorización. Este proceso garantiza una protección suficiente de la confidencialidad, la integridad y la disponibilidad de la información y los sistemas de información. Esto se basa en la categoría de seguridad y el nivel de impacto del sistema (bajo, moderado o alto), así como en la determinación del riesgo. Los controles de seguridad se seleccionan del catálogo de controles de seguridad de NIST SP 800-53 y el sistema se evalúa con respecto a los requisitos de estos controles de seguridad.

El marco NIST 800-53 (Rev. 5) Low-Moderate-High representa los controles de seguridad y los procedimientos de evaluación asociados que se definen en los controles de seguridad recomendados para los sistemas y organizaciones de información federales del NIST SP 800-53, revisión 5. Para cualquier discrepancia que se observe en el contenido entre este marco del NIST SP 800-53 y la última publicación especial del NIST SP 800-53, revisión 5, consulte los documentos oficiales publicados que están disponibles en el Centro de Recursos de Seguridad Informática del NIST.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco NIST 800-53 (Rev. 5) Low-Moderate-High para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos del NIST. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza

a evaluar sus recursos de AWS. Para ello, se basa en los controles definidos en el marco NIST 800-53 (Rev. 5) Low-Moderate-High. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco NIST 800-53 (Rev. 5), Low-Moderate-High son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
NIST 800-53 (Rev. 5) Low-Moderate-High	225	782	280	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_NIST-800-53-Rev.5-Low-Moderate-High.zip.

Los controles de este marco de AWS Audit Manager no tienen por objeto verificar si sus sistemas cumplen con la norma de NIST. Además, no pueden garantizarle que vaya a superar una auditoría

del NIST. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco NIST 800-53 (Rev. 5) Low-Moderate-High. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos del NIST

- Instituto Nacional de Estándares y Tecnología (NIST)
- Centro de recursos de seguridad informática del NIST
- Página de cumplimiento del NIST de AWS

Marco de Ciberseguridad del NIST versión 1.1

AWS Audit Manager proporciona un marco prediseñado que estructura y automatiza las evaluaciones del marco de ciberseguridad del NIST, basándose en las prácticas recomendadas de AWS.

> **Note**
>
> - Para obtener información sobre el marco de Audit Manager compatible con NIST 800-53 (Rev. 5) Low-Moderate-High, consulte NIST 800-53 (Rev. 5) Low-Moderate-High.

- Para obtener información sobre el marco de Audit Manager compatible con NIST SP 800-171 (Rev. 2), consulte NIST SP 800-171 (Rev. 2).

Temas

¿Qué es el marco de ciberseguridad del NIST?

El Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST) se fundó en 1901 y ahora forma parte del Departamento de Comercio de los Estados Unidos. El NIST es uno de los laboratorios de ciencias físicas más antiguos de los Estados Unidos. El Congreso de los Estados Unidos creó la agencia para mejorar lo que en ese momento era una infraestructura de medición de segunda categoría. Las infraestructuras constituían un importante desafío para la competitividad industrial de Estados Unidos, que se había quedado rezagada con respecto a otras potencias económicas como el Reino Unido y Alemania.

Los Estados Unidos dependen del funcionamiento fiable de la infraestructura crítica. Las amenazas de ciberseguridad explotan la creciente complejidad e interconexión de los sistemas de infraestructura crítica. Ponen en riesgo la seguridad, la economía y la seguridad y salud públicas de los Estados Unidos. Al igual que los riesgos financieros y de reputación, el riesgo de ciberseguridad afecta a los resultados de una empresa. Puede aumentar los costos y afectar a los ingresos. Puede perjudicar la capacidad de una organización para innovar y conseguir y mantener clientes. En última instancia, la ciberseguridad puede amplificar la gestión general de riesgos de una organización.

El Marco de Ciberseguridad (Cybersecurity Framework, CSF) del NIST cuenta con el respaldo de los gobiernos y las industrias de todo el mundo como referencia recomendada para su uso por cualquier organización, independientemente de su sector o tamaño. El marco de ciberseguridad del NIST consta de tres componentes principales: el núcleo del marco, los perfiles y los niveles de implementación. El núcleo del marco contiene las actividades y los resultados de ciberseguridad deseados organizados en 23 categorías que cubren la gama de objetivos de ciberseguridad de una organización. Los perfiles contienen la alineación única de una organización con sus requisitos y objetivos organizacionales, su propensión al riesgo y sus recursos, utilizando los resultados deseados del núcleo del marco. Los niveles de implementación describen el grado en que las

prácticas de gestión de riesgos de ciberseguridad de una organización presentan las características definidas en el núcleo del marco.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el Marco de Ciberseguridad del NIST, versión 1.1 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles de acuerdo con los requisitos del NIST y el CSF. Audit Manager actualmente es compatible con el componente principal del marco al ofrecer 56 controles automatizados y 52 controles manuales. Estos controles se corresponden con 23 categorías de ciberseguridad que se definen en el núcleo del marco. Audit Manager no admite los componentes de perfil e implementación de este marco.

También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el Marco de Ciberseguridad del NIST, versión 1.1. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles de Marco de Ciberseguridad del NIST, versión 1.1, son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
Marco de Ciberseguridad del NIST versión 1.1	56	52	23	• AWS Config • AWS Identity and Access Management

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
				• AWS Security Hub

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_NIST-CSF-v1.1.zip.

Los controles que ofrece Audit Manager no pretenden verificar si sus sistemas cumplen con el Marco de Ciberseguridad del NIST. Además, no pueden garantizarle que vaya a superar una auditoría de ciberseguridad del NIST. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco de ciberseguridad del NIST, versión 1.1. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos del NIST

- Instituto Nacional de Estándares y Tecnología (NIST)
- Centro de recursos de seguridad informática del NIST
- Página de cumplimiento del NIST de AWS
- Marco de ciberseguridad del NIST: alinearse con el CSF del NIST en la nube de AWS

NIST SP 800-171 (Rev. 2)

AWS Audit Manager proporciona un marco prediseñado que estructura y automatiza las evaluaciones del estándar de cumplimiento del NIST SP 800-171, basándose en las prácticas recomendadas de AWS.

> **Note**
>
> - Para obtener información sobre el marco de Audit Manager compatible con NIST 800-53 (Rev. 5) Low-Moderate-High, consulte NIST 800-53 (Rev. 5) Low-Moderate-High.
> - Para obtener información sobre el marco de Audit Manager compatible con el marco de ciberseguridad del NIST, versión 1.1, consulte Marco de Ciberseguridad del NIST versión 1.1.

Temas

¿Qué es NIST SP 800-171?

El NIST SP 800-171 se centra en proteger la confidencialidad de la información no clasificada controlada (Controlled Unclassified Information, CUI) en sistemas y organizaciones no federales. Recomienda requisitos de seguridad específicos para lograr ese objetivo. El NIST 800-171 es una publicación que describe los estándares y prácticas de seguridad necesarios para las organizaciones no federales que gestionan la CUI en sus redes. Fue publicada por primera vez en junio de 2015 por el Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology,

NIST). El NIST es una agencia gubernamental de EE. UU. que publicó varios estándares y publicaciones para fortalecer la resiliencia de la ciberseguridad en los sectores público y privado. El NIST 800-171 ha recibido actualizaciones periódicas en función de las ciberamenazas emergentes y las tecnologías cambiantes. La última versión (revisión 2) se publicó en febrero de 2020.

Los controles de ciberseguridad del NIST 800-171 protegen la CUI en las redes de TI de los contratistas y subcontratistas gubernamentales. Define las prácticas y los procedimientos que deben seguir los contratistas gubernamentales cuando sus redes procesan o almacenan la CUI. El NIST 800-171 solo se aplica a las partes de la red de un contratista en las que esté presente la CUI.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco NIST SP 800-171 Rev. 2 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos del NIST. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el marco del NIST SP 800-171 Rev. 2. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco del NIST SP 800-171 Rev. 2 son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
NIST SP 800-171 Rev. 2	66	58	16	• Amazon CloudWatch • Amazon Elastic Compute Cloud

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
				• AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_NIST-SP-800-171-Rev.2.zip.

Los controles de este marco de AWS Audit Manager no tienen por objeto verificar si sus sistemas cumplen con NIST 800-171. Además, no pueden garantizarle que vaya a superar una auditoría del NIST. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener información acerca de cómo crear una evaluación, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco del NIST SP 800-171 Rev. 2. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos del NIST

- Instituto Nacional de Estándares y Tecnología (NIST)
- Centro de recursos de seguridad informática del NIST
- Página de cumplimiento del NIST de AWS

PCI DSS V3.2.1

AWS Audit Manager proporciona un marco prediseñado compatible con PCI DSS v3.2.1.

> **Note**
>
> Para obtener información sobre PCI DSS v4 y el marco de Audit Manager que lo respalda, consulte PCI DSS V4.0.

Temas

- ¿Qué es PCI DSS?
- Utilice este marco para respaldar la preparación de la auditoría
- Más recursos de PCI DSS

¿Qué es PCI DSS?

El estándar de seguridad de los datos del sector de tarjetas de pago (PCI DSS) es un estándar de seguridad de la información propia. Está administrado por el Consejo de Estándares de Seguridad de PCI, que fundaron American Express, Discover Financial Services, JCB International, MasterCard Worldwide y Visa Inc. El PCI DSS se aplica a las entidades que almacenan, procesan o transmiten datos de titulares de tarjetas (CHD) o datos de autenticación sensibles (SAD). Esto incluye, pero no se limita a, comerciantes, procesadores, adquirentes, emisores y proveedores de servicios. Las marcas de tarjetas obligan a utilizar el PCI DSS, que está administrado por el Consejo de Estándares de Seguridad de la Industria de las Tarjetas de Pago.

AWS está certificado como proveedor de servicios de nivel 1 de PCI DSS, que es el nivel de evaluación más alto disponible. La evaluación de conformidad fue realizada por Coalfire Systems Inc., un evaluador de seguridad cualificado (QSA) independiente. El certificado de conformidad (AOC) del PCI DSS y el resumen de responsabilidad están a su disposición en AWS Artifact. Se trata de un portal de autoservicio para acceder a los informes de cumplimiento de AWS a pedido. Inicie sesión en AWS Artifact en la consola de administración de AWS u obtenga más información en Introducción a AWS Artifact.

Puede descargar el estándar PCI DSS de la biblioteca de documentos del Consejo de Estándares de Seguridad de PCI.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco PCI DSS V3.2.1 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos del PCI DSS. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el marco PCI DSS V3.2.1. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco PCI DSS V3.2.1 son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
PCI DSS V3.2.1	175	487	12	• Amazon Elastic Compute Cloud

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
				• AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_PCI-DSS-V3.2.1.zip.

Los controles de este marco de AWS Audit Manager no tienen por objeto verificar si sus sistemas cumplen con la norma de PCI DDS. Además, no pueden garantizarle que vaya a superar una auditoría del PCI DDS. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener información acerca de cómo crear una evaluación, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco PCI DSS V3.2.1. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos de PCI DSS

- Consejo de normas de seguridad de PCI
- Biblioteca de documentos del Consejo de Estándares de Seguridad de PCI.
- AWS Página de cumplimiento para PCI DSS

PCI DSS V4.0

AWS Audit Manager proporciona un marco prediseñado que admite el Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS) versión 4.0.

> **Note**
>
> Para obtener información sobre PCI DSS v3.2.1 y el marco de Audit Manager que lo respalda, consulte PCI DSS V3.2.1.

Temas

¿Qué es PCI DSS?

El Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS) es un estándar global que proporciona una base de requisitos técnicos y operativos para proteger los datos de pago. El PCI DSS v4.0 es la próxima evolución del estándar.

El PCI DSS se desarrolló para fomentar y mejorar la seguridad de los datos de las cuentas de tarjetas de pago. También facilita la adopción generalizada de medidas de seguridad de datos coherentes a nivel mundial. Proporciona una base de requisitos técnicos y operativos diseñados para proteger los datos de las cuentas. Si bien está diseñado específicamente para centrarse en entornos

con datos de cuentas de tarjetas de pago, también puede utilizar el PCI DSS para protegerse contra las amenazas y proteger otros elementos del ecosistema de pagos.

El Consejo de Estándares de Seguridad de PCI (PCI SSC) introdujo muchos cambios entre las versiones 3.2.1 y 4.0. Estas actualizaciones se dividen en tres categorías:

1. Requisitos en evolución: Cambios para garantizar que el estándar esté actualizado con las amenazas y tecnologías emergentes y con los cambios en el sector de pagos. Algunos ejemplos incluyen requisitos o procedimientos de prueba nuevos o modificados, o la eliminación de un requisito.
2. Aclaración o directrices: Actualizaciones en la redacción, la explicación, la definición, las directrices adicionales o las instrucciones para mejorar la comprensión o proporcionar más información y directrices sobre un tema en particular.
3. Estructura o formato: Reorganización del contenido, incluida la combinación, separación y reorganización de los requisitos para alinear el contenido.

Para obtener más información sobre los cambios, consulte el resumen de los cambios de la versión 3.2.1 a la 4.0 del PCI DSS.

Utilice este marco para respaldar la preparación de la auditoría

> **Note**
>
> Este marco estándar utiliza controles consolidados de Security Hub como origen de datos. Para recopilar correctamente las pruebas de los controles consolidados, asegúrese de activar la configuración de los resultados del control consolidado en Security Hub. Para obtener más información sobre el uso de Security Hub como tipo de origen de datos, consulte los controles de AWS Security Hub admitidos por AWS Audit Manager.

Puede utilizar el marco del PCI DSS V4.0 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos del PCI DSS V4.0. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza

a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el marco del PCI DSS V4.0. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
PCI DSS v4.0	152	128	15	• Amazon API Gateway • Amazon CloudFront • Amazon CloudWatch • Amazon DynamoDB • Amazon Elastic Compute Cloud • Amazon OpenSearch Service • Amazon Redshift • Amazon Relationa l Database Service • Amazon SageMaker

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
				• Amazon Simple Storage Service • AWS Backup • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS KMS • AWS Secrets Manager • AWS Security Hub • AWS WAF

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_PCI-DSS-V4.zip.

Los controles de este marco de AWS Audit Manager no tienen por objeto verificar si sus sistemas cumplen con la norma de PCI DDS. Además, no pueden garantizarle que vaya a superar una auditoría del PCI DDS. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener información acerca de cómo crear una evaluación, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco PCI DSS V4. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos de PCI DSS

- Centro de recursos de PCI DSS v4.0
- Consejo de normas de seguridad de PCI
- Biblioteca de documentos del Consejo de Estándares de Seguridad de PCI.
- AWS Página de cumplimiento para PCI DSS
- Conformidad con el Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS) v4.0 según la guía de conformidad de AWS
- Resumen de los cambios de la versión 3.2.1 a la 4.0 del PCI DSS

SOC 2

El SOC 2 es un procedimiento de auditoría que garantiza que los datos de una empresa se gestionen de forma segura. AWS Audit Manager proporciona un marco prediseñado que admite el SOC 2.

Temas

- ¿Qué es SOC 2?
- Utilice este marco para respaldar la preparación de la auditoría
- Más recursos de SOC 2

¿Qué es SOC 2?

Los controles de sistemas y organizaciones (SOC), definidos por el Instituto Estadounidense de Contadores Públicos Certificados (AICPA), son el nombre de un conjunto de informes que se

producen durante una auditoría. Está diseñado para que lo utilicen las organizaciones de servicios (organizaciones que proporcionan sistemas de información como un servicio a otras organizaciones) para emitir informes validados sobre los controles internos de esos sistemas de información a los usuarios de esos servicios. Los informes se centran en los controles agrupados en cinco categorías conocidas como principios del servicio de confianza.

AWS Los informes de SOC son informes de análisis independientes de terceros que muestran cómo AWS logra los controles y objetivos clave de conformidad. La finalidad de estos informes es proporcionarle ayuda a usted y a sus auditores para entender los controles de AWS establecidos como soporte a las operaciones y a la conformidad. Hay cinco informes de los SOC de AWS:

- AWS Informe SOC 1, disponible para los clientes de AWS en AWS Artifact.
- AWS Informe de seguridad, disponibilidad y confidencialidad del SOC 2, disponible para los clientes de AWS en AWS Artifact.
- AWS El informe de seguridad, disponibilidad y confidencialidad del SOC 2 está disponible para los clientes de AWS en AWS Artifact (el alcance incluye únicamente Amazon DocumentDB).
- AWS Informe de privacidad de tipo I del SOC 2, disponible para los clientes de AWS en AWS Artifact.
- AWS Informe de seguridad, disponibilidad y confidencialidad del SOC 3, disponible públicamente como documento técnico.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar este marco como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos del SOC 2. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus recursos de AWS. Lo hace en función de los controles que se definen en el marco. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control	En el ámbito de Servicios de AWS
SOC 2	20	41	20	• Amazon Elastic Compute Cloud • AWS Auto Scaling • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Para revisar las normas de AWS Config que se utilizan como mapeos de origen de datos en este marco estándar, descargue el archivo AuditManager_ConfigDataSourceMappings_SOC2.zip.

Los controles de este marco de AWS Audit Manager no tienen por objeto comprobar si los sistemas cumplen con las normas. Además, no pueden garantizarle que vaya a superar una auditoría. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Puede encontrar este marco en la pestaña Marcos estándar de Biblioteca de marcos en Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Creación de las evaluaciones.

Al utilizar la consola Audit Manager para crear una evaluación a partir de este marco estándar, la lista de Servicios de AWS en el ámbito se selecciona de forma predeterminada y no se puede editar. Esto se debe a que Audit Manager mapea y selecciona automáticamente las origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del SOC 2. Si necesita editar la lista de servicios incluidos en este marco, puede hacerlo mediante las operaciones de API CreateAssessment o UpdateAssessment. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Personalización de un marco existente y Personalización de un control existente.

Más recursos de SOC 2

- AWS Página de cumplimiento de SOC

Biblioteca de control

Puede acceder a los controles y gestionarlos desde la Biblioteca de controles de Audit Manager. Puede ir a la biblioteca de controles en cualquier momento seleccionando Biblioteca de controles en el panel de navegación de la consola Audit Manager.

La biblioteca de controles contiene un catálogo de controles estándar y controles personalizados.

- Los controles estándar son controles predefinidos proporcionados por AWS. Puede ver los detalles de configuración de los controles estándar, pero no puede editarlos ni eliminarlos. Sin embargo, puede personalizar cualquier control estándar para crear uno nuevo que cumpla con sus requisitos específicos.
- Los controles personalizados son controles personalizados suyos que puede definir. Con el control personalizado, puede especificar las fuentes de datos de las que desea recopilar pruebas. A continuación, puede añadir controles personalizados a un marco personalizado.

  Para obtener más información acerca de cómo agregar un control personalizado a un marco personalizado, consulte Biblioteca de marcos. Para obtener más información acerca de cómo crear una evaluación a partir de un marco de Audit Manager, consulte Evaluaciones en AWS Audit Manager.

En esta sección se describe cómo puede crear y gestionar controles personalizados en Audit Manager.

Temas

Acceder a los controles disponibles en AWS Audit Manager

Puede ver todos los controles disponibles en la página de la Biblioteca de controles de la consola Audit Manager. Desde aquí, también puede crear un control personalizado o personalizar un control existente.

También puede ver todos los controles disponibles mediante la API Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

Para ver los controles disponibles (consola)

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Control de biblioteca.
3. Seleccione la pestaña Controles estándar o la pestaña Controles personalizados para ver los controles disponibles.
4. Para mostrar los detalles de un control, elija cualquier nombre de control.

AWS CLI

Para ver los controles disponibles (AWS CLI)

Ejecute el comando list-controls y especifique un `--control-type`. Puede recuperar una lista de controles estándar. O puede recuperar una lista de controles personalizados.

```
aws auditmanager list-controls --control-type Standard
```

```
aws auditmanager list-controls --control-type Custom
```

Audit Manager API

Para ver los controles disponibles (AP)

Utilice la ListControlsoperación y especifique un ControlType. También puede recuperar una lista de controles estándar. O bien, puede devolver una lista de controles personalizados.

Para obtener más información, elija uno de los enlaces anteriores para obtener más información en la referencia de la API deAWS Audit Manager . Esto incluye información sobre cómo usar la `ListControls` operación y los parámetros en uno de los SDK específicos del idioma AWS .

Revisar los detalles de un control

Puede revisar los detalles de un control mediante la consola Audit Manager, la API Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

Para ver los detalles de control (consola)

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, seleccione Biblioteca de controles para ver una lista de los controles disponibles.
3. Seleccione la pestaña Controles estándar o la pestaña Controles personalizados para ver los controles disponibles.
4. Para mostrar los detalles de un control, elija el nombre del control.

Al abrir un control, verá una página de detalles del control. Las secciones de esta página y su contenido se describen a continuación.

Sección de resumen

En esta sección, se proporciona información general acerca del control. Contiene la información siguiente:

- Nombre de control: el nombre del control.
- Tipo de control: especifica si el control es estándar o personalizado.
- Etiquetas: el número de etiquetas que están asociadas con el control.
- Tipos de origen de datos: la cantidad de tipos de fuentes de datos que se utilizan para este control.
- Asignaciones: la cantidad de atributos de mapeo que se utilizan para recuperar datos de un origen de datos.

Si está viendo un control personalizado, también se muestran los siguientes detalles:

- Creado por: la cuenta que creó el control personalizado.
- Fecha de creación: la fecha en que se creó el control personalizado.
- Última actualización: fecha en la que se editó por última vez el control personalizado.

Pestaña Details

Esta pestaña proporciona información general básica sobre el control. Contiene la información siguiente:

- La sección Descripción proporciona una descripción del control.
- La sección Información sobre las pruebas proporciona una descripción de los procedimientos de prueba recomendados para el control.
- La sección Plan de acción describe las acciones recomendadas que se deben seguir si es necesario corregir el control.

Tabla de datos de fuente

Esta pestaña muestra información acerca de los orígenes de datos para el control. Contiene la información siguiente:

- Nombre del origen de datos, que se aplica únicamente a los controles personalizados. Hace referencia al nombre descriptivo que ha asignado a cada origen de datos. Puede usar este nombre para distinguir entre varios orígenes de datos que pertenecen al mismo tipo de origen de datos.
- Tipo de origen de datos: especifica de dónde provienen los datos de la prueba.
  - Si Audit Manager recopila evidencias, el origen de datos puede ser de cuatro tipos: AWS Security Hub, AWS ConfigAWS CloudTrail, o llamadas a la API deAWS .
  - Si carga sus propias evidencias, el tipo de origen de datos es Manual. Una descripción indica si la prueba manual requerida es una carga de archivo o una respuesta de texto.
- Mapeo: este es el atributo de mapeo que se usa para identificar y recuperar datos del origen de datos.
  - Si el tipo de fuente de datos es AWS Config, la asignación es el nombre de una AWS Config regla específica (por ejemplo,). `EC2_INSTANCE_MANAGED_BY_SSM` Audit Manager utiliza este mapeo para informar del resultado de esa verificación de reglas directamente desde AWS Config.
  - Si el tipo de fuente de datos es AWS Security Hub, la asignación es el nombre de un control específico de Security Hub (por ejemplo,`1.1 – Avoid the use of the`

`"root" account`). Audit Manager utiliza esta asignación para informar del resultado del control de seguridad directamente desde Security Hub.

- Si el tipo de fuente de datos son llamadas a la AWS API, la asignación es el nombre de una llamada a la API específica (por ejemplo,`ec2_DescribeSecurityGroups`). Audit Manager utiliza esta asignación para recopilar la respuesta de la API.
- Si la fuente de datos es AWS CloudTrail, el mapeo es el nombre de un CloudTrail evento específico (por ejemplo,`CreateAccessKey`). Audit Manager utiliza este mapeo para recopilar la actividad de los usuarios relacionada de sus CloudTrail registros.

- Frecuencia: especifica la frecuencia con la que Audit Manager recopila pruebas del origen de datos. La frecuencia varía según el tipo del origen de datos. Para obtener más información, elija el valor de la columna o consulte Frecuencia de recolección de evidencias.

Pestaña de etiquetas

Esta pestaña enumera las etiquetas que están asociadas con el control. Contiene la información siguiente:

- Clave: la clave de la etiqueta (por ejemplo, un estándar, un reglamento o una categoría de cumplimiento).
- Valor: el valor de la etiqueta.

AWS CLI

Para ver los detalles del control (AWS CLI)

1. Para identificar el control que desea revisar, ejecute el comando list-controls y especifique un `--control-type`. Puede recuperar una lista de controles estándar. O puede recuperar una lista de controles personalizados.

   En el siguiente ejemplo, sustituya el *`texto del marcador`* de posición por uno `Custom` o uno `Standard`.

   ```
   aws auditmanager list-controls --control-type Custom/Standard
   ```

   La respuesta devuelve una lista de controles. Busque el control que desea revisar y tome nota del ID de control y el nombre de recurso de Amazon (ARN).
2. Para obtener los detalles del control, ejecute el comando get-control y especifique el `--control-id`.

En el siguiente ejemplo, reemplace cada *placeholder text* con su propia información.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Los detalles de control se devuelven en formato JSON. Para comprender estos datos, consulte el Resultado de get-control en la Referencia de comando deAWS CLI .

3. Para ver las etiquetas de un control, utilice el list-tags-for-resourcecomando y especifique `--resource-arn` las del control.

   En el siguiente ejemplo, reemplace cada *placeholder text* con su propia información:

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Para obtener más información acerca del etiquetado en Audit Manager, consulte Etiquetado de recursos de AWS Audit Manager.

Audit Manager API

Para ver los detalles del control (API)

1. Para identificar el control que desea revisar, utilice la ListControlsoperación y especifique un ControlType. También puede recuperar una lista de controles estándar. O bien, puede devolver una lista de controles personalizados.

   En la respuesta, busque el control que desea revisar y tome nota del ID de control y el nombre de recurso de Amazon (ARN).

2. Para obtener los detalles del control, utilice la GetControloperación. En la solicitud, especifique el Id del control que obtuvo en el paso 1.

   Los detalles de control se devuelven en formato JSON. Para entender estos datos, consulta los elementos de GetControl respuesta en la referencia de laAWS Audit Manager API.

3. Para ver las etiquetas del control, utilice la ListTagsForResourceoperación. En la solicitud, especifique el resourceArn que obtuvo en el paso 1.

Para obtener más información acerca del etiquetado de recursos en Audit Manager, consulte los recursos de Etiquetado. AWS Audit Manager

Para más información sobre estas operaciones de la API, consulte cualquiera de los enlaces anteriores en la referencia de la API deAWS Audit Manager . Esto incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los SDK específicos del idioma AWS .

Creación de un control personalizado

Puede utilizar controles personalizados para recopilar pruebas de los orígenes de datos específicos que defina.

Al igual que los controles estándar, los controles personalizados recopilan pruebas de forma continua cuando están activos en las evaluaciones. También puede añadir pruebas manuales a cualquier control personalizado que cree. Cada prueba se convierte en un registro que le ayuda a demostrar el cumplimiento de los requisitos de su control personalizado.

A continuación, se muestran algunos ejemplos de cómo puede usar los controles personalizados:

Usar un control existente como punto de partida

Puede personalizar cualquier control en Audit Manager. Se trata de una buena opción si un control existente cumple, más o menos, su objetivo, pero desea ampliar su orientación o ajustar algunos atributos para adaptarlo a sus necesidades específicas. Por ejemplo, puede cambiar la frecuencia con la que un control recopila pruebas y, a continuación, cambiar el nombre del control para reflejar esto.

Crear un control personalizado para las auditorías internas

Para respaldar las auditorías internas, puede crear un control personalizado diseñado específicamente que no esté relacionado con ningún marco o reglamento de cumplimiento específico. Esto le da la libertad de adaptar los requisitos de control a un área en particular o de recopilar pruebas a partir de un recurso específico de la empresa. Por ejemplo, puede crear un control personalizado que utilice AWS Config las reglas personalizadas de su organización como fuente de datos para la recopilación de pruebas.

Cree una pregunta de evaluación de riesgos para el proveedor

Puede usar controles personalizados para respaldar la gestión de las evaluaciones de riesgo de los proveedores. Cada control que cree puede representar una pregunta de evaluación de riesgos

individual. En este caso, el nombre del control puede ser una pregunta y puede proporcionar una respuesta cargando un archivo o introduciendo una respuesta de texto como prueba manual.

Hay dos formas de crear un control personalizado. Puede crear un control nuevo desde cero o personalizar un control existente.

Temas

- Creación de un nuevo control personalizado desde cero
- Personalizar un control existente

Creación de un nuevo control personalizado desde cero

Puede crear un nuevo control personalizado desde cero siguiendo estos pasos.

> **Important**
>
> Le recomendamos encarecidamente que no incluya nunca información de identificación confidencial en los campos de formato libre como Detalles de control, Información de prueba o Plan de acción. Si crea controles personalizados que contienen información confidencial, no podrá compartir ninguno de sus marcos personalizados que contengan estos controles.

Temas

- Paso 1: especificar los detalles de control
- Paso 2: configurar orígenes de datos
- Paso 3 (opcional): defina un plan de acción
- Paso 4: revisar y crear el control
- ¿Qué tengo que hacer ahora?

Paso 1: especificar los detalles de control

Comience por especificar los detalles de su control personalizado.

Para especificar los detalles del control

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Biblioteca de controles y, a continuación, elija Crear control personalizado.
3. En Detalles del control, introduzca la siguiente información sobre el control.
   - Control: introduzca un nombre descriptivo, un título o una pregunta de evaluación de riesgos. Este valor le ayuda a identificar el control en la biblioteca de controles.
   - Descripción (opcional): introduzca los detalles para ayudar a otros a entender el objetivo del control. Esta descripción aparece en la página de detalles del control.
4. En Información de prueba, introduzca los pasos recomendados para probar el control.
5. En Etiquetas, elija Añadir nueva etiqueta para asociar una etiqueta al control. Puede especificar una clave para cada etiqueta que describa mejor el marco de conformidad compatible con este control. La clave de etiqueta es obligatoria y se puede utilizar como criterio de búsqueda al buscar este control en la biblioteca de controles.
6. Elija Siguiente.

Paso 2: configurar orígenes de datos

A continuación, defina hasta 10 orígenes de datos. Un origen de datos determina de dónde recopila las pruebas su control personalizado.

Si desea recopilar pruebas automatizadas, cada origen de datos debe incluir un tipo de origen de datos y un mapeo del origen de datos. Estos detalles se relacionan con su AWS uso e indican a Audit Manager de dónde debe recopilar las pruebas. Si, en lugar de ello, desea proporcionar sus propias pruebas, asignará un nombre al origen de datos y, a continuación, elegirá una opción de prueba manual.

> **Important**
>
> Para utilizar AWS Config correctamente Security Hub como fuentes de datos automatizadas, asegúrese de hacer lo siguiente:
>
> - Siga las instrucciones para configurar AWS Configy configurar Security Hub para su uso con Audit Manager.

- Incluya ambos AWS Config y Security Hub como servicios incluidos en su evaluación.

A continuación, Audit Manager puede recopilar pruebas cada vez que se realice una evaluación de las AWS Config reglas o los controles del Security Hub que especifique en este paso.

Para configurar orígenes de datos

1. En Nombre del origen de datos, sustituya el texto del marcador de posición por un nombre descriptivo para el origen de datos.
2. En Método de recopilación de pruebas, elija cómo desea recopilar las pruebas para este control.

   a. Si desea que Audit Manager recopile pruebas, elija Automatizado y siga estos pasos:

      - En Tipo de origen de datos, especifique de dónde recopila Audit Manager las pruebas automatizadas.
        - Para AWS CloudTrail, elija una palabra clave para el nombre del evento en la lista desplegable.
        - Para AWS Config, seleccione un tipo de regla y, a continuación, elija una palabra clave identificadora de regla en la lista desplegable.
        - Para AWS Security Hub, elija un control de Security Hub de la lista desplegable.
        - Para las llamadas a la API deAWS , elija una llamada a la API y, a continuación, seleccione una frecuencia de recopilación de evidencias.

      > **Tip**
      >
      > Para obtener una descripción general de cada tipo de origen de datos y consejos de solución de problemas relacionados, consulte Descripción general de los orígenes de datos automatizadas.
      > Si necesita validar la configuración del origen de datos con un experto en el dominio, defina el método de recopilación de pruebas como manual de momento. De esta forma, puede crear el control y añadirlo a un marco ahora y, a continuación, editar el control según sea necesario más adelante.

b. Si desea proporcionar sus propias pruebas, elija Manual y seleccione una opción de prueba manual.

- Carga de archivos: seleccione esta opción si el control requiere documentación como prueba.
- Respuesta de texto: seleccione esta opción si el control requiere una respuesta a una pregunta de evaluación de riesgos.

3. (Opcional) En Detalles adicionales, introduzca una descripción del origen de datos y una descripción de la solución de problemas.
4. (Opcional) Para agregar otro origen de datos, elija Add data source (Agregar origen de datos) y, a continuación, repita los pasos 1-3.
5. (Opcional) Para eliminar un origen de datos, seleccione Eliminar en la parte superior del cuadro de configuración del origen de datos.
6. Cuando haya terminado, elija Siguiente.

Paso 3 (opcional): defina un plan de acción

A continuación, especifique las acciones que se deben tomar si es necesario corregir este control.

Para definir un plan de acción

1. En Título, introduzca un título descriptivo para el plan de acción.
2. En Instrucciones del plan de acción, introduzca instrucciones detalladas para el plan de acción.
3. Elija Siguiente.

Paso 4: revisar y crear el control

Revisión de la información de la pila. Para modificar la información de un paso, seleccione Editar.

Cuando haya terminado, elija Crear.

¿Qué tengo que hacer ahora?

Tras crear un nuevo control personalizado, puede añadirlo a un marco personalizado. Para obtener más información, consulte Crear un marco personalizado o Editar un marco personalizado.

Tras añadir el control personalizado a un marco personalizado, puede crear una evaluación a partir de ese marco personalizado y empezar a recopilar pruebas. Para obtener más información, consulte Creación de las evaluaciones.

Para obtener sugerencias acerca de la solución de problemas, consulte Solución de problemas de control y conjunto de control.

Personalizar un control existente

En lugar de crear un control personalizado desde cero, puede utilizar un control existente como punto de partida y personalizarlo según sus necesidades. Al hacerlo, el control existente permanece en la biblioteca de controles y se crea un nuevo control personalizado con sus ajustes personalizados.

Puede seleccionar cualquier control existente para personalizarlo. Puede ser un control estándar o un control personalizado.

> **Important**
>
> Le recomendamos encarecidamente que no incluya nunca información de identificación confidencial en los campos de formato libre como Detalles de control, Información de prueba o Plan de acción. Si crea controles personalizados que contienen información confidencial, no podrá compartir ninguno de sus marcos personalizados que contengan estos controles.

Temas

Paso 1: especificar los detalles de control

Los detalles del control se heredan del control original. Revise y modifique estos detalles según sea necesario.

Para especificar los detalles del control

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Control de costos.
3. Seleccione el control que desee personalizar y, a continuación, elija Personalizar el control existente.
4. Especifique el nuevo nombre del control y elija Personalizar.
5. En Detalles del control, personalice los detalles del control según sea necesario.
6. En Información de pruebas, personalice la información de las pruebas según sea necesario.
7. En Etiquetas, personalice las etiquetas según sea necesario.
8. Elija Siguiente.

Paso 2: configurar orígenes de datos

Los orígenes de datos se heredan del control original. Puede cambiar, añadir o eliminar los orígenes de datos según sea necesario.

> **Important**
>
> Para utilizar AWS Config correctamente Security Hub como fuentes de datos automatizadas, asegúrese de hacer lo siguiente:
>
> - Siga las instrucciones para configurar AWS Configy configurar Security Hub para su uso con Audit Manager.
> - Incluya ambos AWS Config y Security Hub como servicios incluidos en su evaluación.
>
> A continuación, Audit Manager puede recopilar pruebas cada vez que se realice una evaluación de las AWS Config reglas o los controles del Security Hub que especifique en este paso.

Para configurar orígenes de datos

1. En Nombre del origen de datos, personalice el nombre del origen de datos según sea necesario.

2. En Método de recopilación de pruebas, personalice la selección según sea necesario.

   a. Si desea que Audit Manager recopile pruebas, elija Automatizado y siga estos pasos:

      - En Tipo de origen de datos, revise de dónde recopila Audit Manager las pruebas automatizadas y modifíquelas según sea necesario.
        - Para AWS CloudTrail, elija una palabra clave para el nombre del evento en la lista desplegable.
        - Para AWS Config, seleccione un tipo de regla y, a continuación, elija una palabra clave identificadora de regla en la lista desplegable.
        - Para AWS Security Hub, elija un control de Security Hub de la lista desplegable.
        - Para las llamadas a la API deAWS , elija una llamada a la API y, a continuación, seleccione una frecuencia de recopilación de evidencias.

      > **Tip**
      >
      > Para obtener una descripción general de cada tipo de origen de datos y consejos de solución de problemas relacionados, consulte Descripción general de los orígenes de datos automatizadas.
      > Si necesita validar la configuración del origen de datos con un experto en el dominio, defina el método de recopilación de pruebas como manual de momento. De esta forma, puede crear el control y añadirlo a un marco ahora y, a continuación, editar el control según sea necesario más adelante.

   b. Si desea proporcionar sus propias pruebas, elija Manual y seleccione una opción de prueba manual.

      - Carga de archivos: seleccione esta opción si el control requiere documentación como prueba.
      - Respuesta de texto: seleccione esta opción si el control requiere una respuesta a una pregunta de evaluación de riesgos.

3. (Opcional) En Detalles adicionales, realice los cambios necesarios en la descripción del origen de datos o en la descripción de la solución de problemas.
4. (Opcional) Para agregar otro origen de datos, elija Añadir origen de datos.
5. (Opcional) Para eliminar un origen de datos, elija Eliminar.
6. Elija Siguiente.

Paso 3: (opcional): definir un plan de acción

El plan de acción se hereda del control original. Puede editar este plan de acción según sea necesario.

Para definir un plan de acción

1. Revise en Título el título del plan de acción y personelícelo según sea necesario.
2. En Instrucciones del plan de acción, revise y personalice las instrucciones según sea necesario.
3. Elija Siguiente.

Paso 4: revisar y crear el control

Revisión de la información de la pila. Para modificar la información de un paso, seleccione Editar. Cuando haya terminado, elija Crear.

¿Qué tengo que hacer ahora?

Tras crear un nuevo control personalizado, puede añadirlo a un marco personalizado. Para obtener más información, consulte Crear un marco personalizado y Editar un marco personalizado.

Tras añadir un control personalizado a un marco personalizado, puede crear una evaluación a partir de ese marco personalizado y empezar a recopilar pruebas. Para obtener más información, consulte Creación de las evaluaciones.

Si necesita editar un control personalizado, consulteEditar un control personalizado.

Para obtener sugerencias acerca de la solución de problemas, consulte Solución de problemas de control y conjunto de control.

Editar un control personalizado

Puede editar un control personalizado en Audit Manager siguiendo estos pasos.

Temas

- Paso 1: editar los detalles de control
- Paso 2: editar orígenes de datos

- Paso 3: (opcional) editar un plan de acción
- Paso 4: revisar y actualizar el control

Paso 1: editar los detalles de control

Comience por revisar y editar los detalles del control según sea necesario.

Para editar los detalles de los controles

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Biblioteca de controles y, a continuación, elija la pestaña Controles personalizados.
3. Seleccione el control que desea modificar y elija Editar.
4. En Detalles de control, edite los detalles del control según sea necesario.
5. En Información de pruebas, edite la información de prueba recomendada según sea necesario.
6. Elija Siguiente.

> **Tip**
>
> Para editar las etiquetas de un control, abra el control y seleccione la pestaña Etiquetas. Allí puede ver y editar las etiquetas asociadas al control.

Paso 2: editar orígenes de datos

A continuación, puede editar, quitar o agregar orígenes de datos para el control.

> **Important**
>
> Para utilizar AWS Config correctamente Security Hub como fuentes de datos automatizadas, asegúrese de hacer lo siguiente:
>
> - Siga las instrucciones para configurar AWS Configy configurar Security Hub para su uso con Audit Manager.
> - Incluya ambos AWS Config y Security Hub como servicios incluidos en su evaluación.

A continuación, Audit Manager puede recopilar pruebas cada vez que se realice una evaluación de las AWS Config reglas o los controles del Security Hub que especifique en este paso.

Para editar orígenes de datos

1. Revise en Nombre del origen de datos el nombre actual y edítelo según sea necesario.
2. Revise en Método de recopilación de pruebas revise la selección actual y edítela según sea necesario.

   a. Si desea que Audit Manager recopile pruebas, elija Automatizado y siga estos pasos:

      - Revise en Tipo de origen de datos de dónde recopila Audit Manager las pruebas automatizadas y edítelas según sea necesario.
        - Para AWS CloudTrail, elija una palabra clave para el nombre del evento en la lista desplegable.
        - Para AWS Config, seleccione un tipo de regla y, a continuación, elija una palabra clave identificadora de regla en la lista desplegable.
        - Para AWS Security Hub, elija un control de Security Hub de la lista desplegable.
        - Para las llamadas a la API deAWS , elija una llamada a la API y, a continuación, seleccione una frecuencia de recopilación de evidencias.

      > **Tip**
      >
      > Para obtener una descripción general de cada tipo de origen de datos y consejos de solución de problemas relacionados, consulte Descripción general de los orígenes de datos automatizadas.

   b. Si desea proporcionar sus propias pruebas, elija Manual y seleccione una opción de prueba manual.

      - Carga de archivos: seleccione esta opción si el control requiere documentación como prueba.
      - Respuesta de texto: seleccione esta opción si el control requiere una respuesta a una pregunta de evaluación de riesgos.

3. (Opcional) En Detalles adicionales, realice los cambios necesarios en la descripción del origen de datos o en la descripción de la solución de problemas.
4. (Opcional) Para agregar otro origen de datos, elija Añadir origen de datos.
5. (Opcional) Para eliminar un origen de datos, elija Eliminar.
6. Elija Siguiente.

Paso 3: (opcional) editar un plan de acción

A continuación, revise y edite el plan de acción opcional.

Para editar un plan de acción

1. En Título, edite el título según sea necesario.
2. En Instrucciones del plan de acción, edite las instrucciones según sea necesario.
3. Elija Siguiente.

Paso 4: revisar y actualizar el control

Revisión de la información de la pila. Para modificar la información de un paso, seleccione Editar.

Cuando haya finalizado, elija Save changes (Guardar cambios).

> **Note**
>
> Tras editar un control, los cambios se aplican de la siguiente manera en todas las evaluaciones activas que incluyen el control:
>
> - En el caso de los controles con llamadas a laAWS API como tipo de origen de datos, los cambios se aplican a las 00:00 UTC del día siguiente.
> - Los cambios surtirán efecto de inmediato en los demás controles.

Eliminación de un control personalizado

Puede utilizar la biblioteca de controles para eliminar un control personalizado no deseado. Tras eliminar un control, dejará de aparecer en la biblioteca de controles. También puede eliminar los

controles personalizados mediante la API Audit Manager o AWS Command Line Interface (AWS CLI).

> **Important**
>
> Al eliminar un control personalizado se elimina el control de todos los marcos o evaluaciones personalizados con los que esté relacionado actualmente. Por lo tanto, Audit Manager dejará de recopilar pruebas para ese control personalizado en todas sus evaluaciones. Esto incluye las evaluaciones que haya creado previamente antes de eliminar el control personalizado.

Audit Manager console

Para eliminar un control personalizado (consola)

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija Biblioteca de controles y, a continuación, elija la pestaña Controles personalizados.
3. Seleccione el control que desea eliminar y luego elija Eliminar.
4. En la ventana emergente que aparece, seleccione Eliminar para confirmar la eliminación.

AWS CLI

Para eliminar un control personalizado (AWS CLI)

1. En primer lugar, identifique el control personalizado que desea eliminar. Para ello, ejecute el comando list-controls y especifique el `--control-type` como `Custom`.

   ```
   aws auditmanager list-controls --control-type Custom
   ```

   La respuesta devuelve una lista de controles personalizados. Busque el control que desee eliminar y anote el ID del control.

2. A continuación, ejecute el comando delete-control y utilice el parámetro `--control-id` para especificar el control que desee eliminar.

   En el siguiente ejemplo, reemplace cada *`placeholder text`* con su propia información.

```
aws auditmanager delete-control --control-id a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111
```

Audit Manager API

Para eliminar un control personalizado (API)

1. Utilice la ListControlsoperación y especifique el ControlType comoCustom. En la respuesta, busque el control que desee eliminar y anote el ID del control.
2. Utilice la DeleteControloperación para eliminar el control personalizado. En la solicitud, utilice el parámetro Id de control para especificar el control que desea eliminar.

Para más información sobre estas operaciones de la API, consulte cualquiera de los enlaces anteriores en la referencia de la API deAWS Audit Manager . Esto incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los SDK específicos del idioma AWS .

Cambiar la frecuencia de recopilación de evidencias para un control

AWS Audit Manager recopila evidencia de múltiples fuentes de datos con diferentes frecuencias. La frecuencia de recopilación de evidencias compatibles depende del tipo de prueba que se recopile para el control.

- En el caso de las llamadas a la API deAWS , Audit Manager recopila pruebas mediante una llamada de descripción de la API a otro Servicio de AWS. Puede especificar la frecuencia de recopilación de evidencias directamente en Audit Manager (solo para controles personalizados).
- AWS ConfigEn efecto, Audit Manager informa del resultado de una comprobación de conformidad directamente desde AWS Config. La frecuencia sigue los activadores que se definen en la regla de AWS Config .
- Audit Manager informa del resultado de una comprobación de conformidad directamente desde el Security Hub al usarse con AWS Security Hub. La frecuencia sigue la programación de comprobación de Security Hub.
- Pues AWS CloudTrail, Audit Manager recopila pruebas de forma continua de CloudTrail. No puede cambiar la frecuencia de este tipo de prueba.

En las siguientes secciones se proporciona más información sobre la frecuencia de recopilación de evidencias para cada tipo de origen de datos de control y sobre cómo cambiarla (si procede).

Temas

Instantáneas de configuración a partir de llamadas a la AWS API

> **Note**
>
> Lo siguiente se aplica solo a los controles personalizados. No puede cambiar la frecuencia de recopilación de evidencias para un control estándar que utiliza llamadas a la API como origen de datos.

Si un control personalizado utiliza llamadas a la AWS API como tipo de fuente de datos, puede cambiar la frecuencia de recopilación de pruebas en Audit Manager siguiendo estos pasos.

Para cambiar la frecuencia de recopilación de evidencias de un control personalizado con un origen de datos de llamadas a la API

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación, elija la Biblioteca de controles y, a continuación, elija la pestaña Controles personalizados.
3. Elija la ACL web que desee editar y, a continuación, seleccione Editar.
4. En la página Editar detalles del control, seleccione Siguiente.
5. Busque el cuadro de origen de datos que desea editar y compruebe que la siguiente información es correcta:
   - El método de recopilación de pruebas es automático.
   - El tipo de origen de datos son las llamadas a la API deAWS .
   - La llamada a la API seleccionada es para la que desea cambiar la frecuencia.

6. En Frecuencia, elija la frecuencia con la que desea recopilar pruebas para el control personalizado.
7. Repita los pasos 5 y 6 según sea necesario para cualquier origen de datos de llamadas a la API adicional que desee editar.
8. Elija Siguiente.
9. En la página Editar un plan de acción, seleccione Siguiente.
10. Revise en la página Revisar y actualizar el control la información del control personalizado. Para modificar la información de un paso, seleccione Editar.
11. Cuando haya finalizado, elija Save changes (Guardar cambios).

Los cambios se aplicarán a las 00:00 UTC del día siguiente en todas las evaluaciones activas que incluyan el control al editar un control con llamadas a la API deAWS como tipo de origen de datos.

Comprobaciones de cumplimiento de AWS Config

> **Note**
>
> Lo siguiente se aplica tanto a los controles estándar como a los controles personalizados que utilizan Reglas de AWS Config como origen de datos.

Si un control se utiliza AWS Config como tipo de fuente de datos, no puede cambiar la frecuencia de recopilación de pruebas directamente en Audit Manager. Esto se debe a que la frecuencia sigue los activadores que se definen en la AWS Config regla.

Existen dos tipos de desencadenantes para Reglas de AWS Config:

1. Cambios de configuración: AWS Config ejecuta evaluaciones de la regla cuando se crean, modifican o eliminan determinados tipos de recursos.
2. Periódico: AWS Config ejecuta las evaluaciones de la regla con la frecuencia que elija (por ejemplo, cada 24 horas).

Para obtener más información sobre los activadores Reglas de AWS Config, consulta los tipos de activadores en la Guía paraAWS Config desarrolladores.

Para obtener instrucciones sobre cómo administrar Reglas de AWS Config, consulte Administrar AWS Config las reglas.

Comprobaciones de cumplimiento desde Security Hub

> **Note**
>
> Lo siguiente se aplica tanto a los controles estándar como a los controles personalizados que utilizan las comprobaciones de Security Hub como origen de datos.

Si un control utiliza Security Hub como tipo de origen de datos, no puede cambiar la frecuencia de recopilación de evidencias directamente en Audit Manager. Esto se debe a que la frecuencia sigue la programación de las comprobaciones de Security Hub.

- Las comprobaciones periódicas se ejecutan automáticamente en las 12 horas posteriores a la última ejecución. No puede cambiar la periodicidad.
- Las comprobaciones activadas por cambios se ejecutan cuando el recurso asociado cambia de estado. Incluso si el recurso no cambia de estado, la actualización a tiempo para las comprobaciones activadas por cambios se actualiza cada 18 horas. Esto ayuda a indicar que el control sigue habilitado. En general, Security Hub utiliza reglas activadas por cambios siempre que sea posible.

Para obtener más información, consulte el programa de ejecución de los controles de seguridad en la Guía del usuario deAWS Security Hub .

Registros de actividad de los usuarios de AWS CloudTrail

> **Note**
>
> Lo siguiente se aplica tanto a los controles estándar como a los controles personalizados que utilizan los registros de actividad de los usuarios de AWS CloudTrail como origen de datos.

No puede cambiar la frecuencia de recopilación de pruebas para los controles que utilizan los registros de actividad CloudTrail como tipo de fuente de datos. Audit Manager recopila este tipo CloudTrail de evidencia de forma continua. La frecuencia es continua porque la actividad de los usuarios puede ocurrir en cualquier momento del día.

Origen de datos de control compatibles para pruebas automatizadas

Al crear un control personalizado en AWS Audit Manager, puede configurarlo para recopilar pruebas automatizadas de los siguientes tipos de fuentes de datos:

- AWS CloudTrail
- AWS Security Hub
- AWS Config
- AWS Llamadas a la API

En los siguientes temas se resume cada uno de estos tipos de fuentes de datos automatizadas y se enumeran AWS Security Hub los controles, AWS Config reglas y llamadas a la AWS API específicos que admite Audit Manager.

Temas

Descripción general de los orígenes de datos automatizadas

En la siguiente tabla se proporciona información general de cada tipo de orígenes de datos automatizada.

Data source type	Descripción	Frecuencia de recolección de evidencias	Para usar este tipo de origen de datos...	Cuando este control está activo en una evaluación...	Consejos relacionados para la solución de problemas
AWS CloudTrail	Realiza un seguimiento de la actividad de un usuario específico.	Continuo.	Seleccionar la lista de nombres de eventos compatibles.	Audit Manager filtra los CloudTrail registros en función de la palabra clave que elija. Los resultados se importan como evidencia de la Actividad del usuario.	Mi evaluación no consiste en recopilar pruebas de la actividad de los usuarios de AWS CloudTrail
AWS Config	Captura una instantánea del estado de seguridad de sus recursos al informar	Se basa en los factores desencadenantes definidos en la AWS Config regla.	Seleccione un tipo regla y, a continuación, elija una regla. • Seleccione las reglas administradas desde la lista de palabras clave de reglas administradas compatibles. • Selecciónela las reglas personalizadas desde la	Audit Manager obtiene los resultados de esta regla directamente de AWS Config. El resultado se importa como evidencia de Verificación de conformidad.	Mi evaluación no consiste en recopilar pruebas de control de

Data source type	Descripción	Frecuencia de recolección de evidencias	Para usar este tipo de origen de datos...	Cuando este control está activo en una evaluación...	Consejos relacionados para la solución de problemas
	sobre los resultados obtenidos AWS Config.		lista de reglas disponibles.		conformidad de AWS Config AWS Config problemas de integración
AWS Security Hub	Captura una instantánea del estado de seguridad de sus recursos mediante el informe de los resultados de Security Hub.	Según la programación de la comprobación de Security Hub.	Seleccione de la lista de identificadores de control de Security Hub compatibles.	Audit Manager obtiene el resultado del control de seguridad directamente desde Security Hub. El resultado se importa como evidencia de Verificación de conformidad.	Mi evaluación no consiste en recopilar pruebas de control de conformidad de AWS Security Hub

Data source type	Descripción	Frecuencia de recolección de evidencias	Para usar este tipo de origen de datos...	Cuando este control está activo en una evaluación...	Consejos relacionados para la solución de problemas
AWS llamada a la API	Toma una instantánea de la configuración de los recursos directamente mediante una llamada a la API especificada Servicio de AWS.	Diariamente, semanalmente o mensualmente.	Seleccione una opción de la lista de llamadas a la API compatibles y, a continuación, seleccione la frecuencia que prefiera.	Audit Manager realiza la llamada a la API en función de la frecuencia que especifique. La respuesta se importa como evidencia de Datos de configuración.	Mi evaluación no consiste en recopilar pruebas de datos de configuración para una llamada a la API de AWS

Reglas de AWS Config con el apoyo de AWS Audit Manager

Puede usar Audit Manager para capturar AWS Config las evaluaciones como evidencia para las auditorías. Al crear o editar un control personalizado, puede especificar una o más AWS Config reglas como mapeo de fuentes de datos para la recopilación de pruebas. AWS Config realiza comprobaciones de conformidad en función de estas reglas, y Audit Manager informa de los resultados como evidencia de las comprobaciones de conformidad.

Además de las reglas gestionadas, también puede asignar sus reglas personalizadas a un origen de datos de control.

> **Note**
>
> - Audit Manager no recopila pruebas de las reglas de AWS Config vinculadas a servicios, con la excepción de las reglas vinculadas a servicios de los paquetes de conformidad y de AWS Organizations. Para obtener más información, consulta la sección de resolución de problemas de la guía.
> - Audit Manager no gestiona AWS Config las reglas por usted. Antes de iniciar la recopilación de pruebas, le recomendamos que revise los parámetros actuales de AWS Config la regla. A continuación, valide esos parámetros según los requisitos del marco que haya elegido. Si es necesario, puede actualizar los parámetros de una regla de AWS Configpara que se ajusten a los requisitos del marco. Esto ayudará a garantizar que sus evaluaciones recopilan las pruebas de control de conformidad correctas para ese marco.
>
> Supongamos, por ejemplo, que está creando una evaluación para CIS v1.2.0. Este marco tiene un control denominado 1.9: asegúrese de que la política de contraseñas de IAM exija una longitud mínima de 14 o más. En AWS Config, la iam-password-policyregla tiene un `MinimumPasswordLength` parámetro que comprueba la longitud de la contraseña. El valor predeterminado para este parámetro es 14 caracteres. Por lo tanto, la regla concuerda con los requisitos de control establecidos. Si no utiliza el valor de parámetro predeterminado, asegúrese de que sea igual o superior al requisito de 14 caracteres establecido en CIS v1.2.0. Puede encontrar los detalles de los parámetros predeterminados de cada regla administrada en la documentación deAWS Config.

Temas

- Uso de reglas AWS Config gestionadas con Audit Manager
- Uso de reglas AWS Config personalizadas con Audit Manager
- Solución de problemas AWS Config de integración con Audit Manager

Uso de reglas AWS Config gestionadas con Audit Manager

Audit Manager admite actualmente 326 reglas AWS Config gestionadas. Puede utilizar cualquiera de las siguientes palabras clave identificadoras de reglas administradas al configurar un origen de

datos para un control personalizado. Para obtener más información sobre cualquiera de las reglas administradas que se enumeran a continuación, elija un elemento de la lista o consulte las reglas administradas deAWS Config en la Guía del usuario deAWS Config .

> **Tip**
>
> Asegúrese de buscar una de las siguientes palabras clave identificadoras de reglas en vez de el nombre de la regla al elegir una regla gestionada en la consola de Audit Manager durante la creación de un control personalizado. Para obtener información sobre la diferencia entre el nombre de la regla, el identificador de la regla y cómo encontrar el identificador de una regla administrada, consulte la sección de solución de problemas de esta guía del usuario.

Palabras clave de reglas AWS Config administradas compatibles

- ACCESS_KEYS_ROTATED
- ACCOUNT_PART_OF_ORGANIZATIONS
- ACM_CERTIFICATE_EXPIRATION_CHECK
- ACM_CERTIFICATE_RSA_CHECK
- ALB_DESYNC_MODE_CHECK
- ALB_HTTP_DROP_INVALID_HEADER_ENABLED
- ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK
- ALB_WAF_ENABLED
- API_GW_ASOCIADA_CON_WAF
- API_GW_CACHE_ENABLED_AND_ENCRYPTED
- API_GW_ENDPOINT_TYPE_CHECK
- API_GW_EXECUTION_LOGGING_ENABLED
- API_GW_SSL_ENABLED
- API_GW_XRAY_ENABLED
- API_GWV2_ACCESS_LOGS_ENABLED
- API_GWV2_AUTHORIZATION_TYPE_CONFIGURED
- APPROVED_AMIS_BY_ID

Palabras clave de reglas AWS Config administradas compatibles

- APPROVED_AMIS_BY_TAG
- APPSYNC_ASSOCIATED_WITH_WAF
- APPSYNC_CACHE_ENCRYPTION_AT_REST
- APPSYNC_LOGGING_ENABLED
- AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED
- AURORA_MYSQL_BACKTRACKING_ENABLED
- AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- AUTOSCALING_CAPACITY_REBALANCING
- AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED
- AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT
- AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED
- AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2
- AUTOSCALING_LAUNCH_TEMPLATE
- AUTOSCALING_MULTIPLE_AZ
- AUTOSCALING_MULTIPLE_INSTANCE_TYPES
- BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
- BACKUP_RECOVERY_POINT_ENCRYPTED
- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED
- CLB_DESYNC_MODE_CHECK
- CLB_MULTIPLE_AZ
- CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED
- CLOUD_TRAIL_ENABLED
- CLOUD_TRAIL_ENCRYPTION_ENABLED
- CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED
- CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK
- CLOUDFORMATION_STACK_NOTIFICATION_CHECK
- CLOUDFRONT_ACCESSLOGS_ENABLED

Palabras clave de reglas AWS Config administradas compatibles

- CLOUDFRONT_ASSOCIATED_WITH_WAF
- CERTIFICADO CLOUDFRONT_CUSTOM_SSL_CERTIFICATE
- CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED
- CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS
- CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED
- CLOUDFRONT_ORIGIN_FAILOVER_ENABLED
- CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED
- CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET
- CLOUDFRONT_SECURITY_POLICY_CHECK
- CLOUDFRONT_SNI_ENABLED
- CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED
- CLOUDFRONT_VIEWER_POLICY_HTTPS
- CLOUDTRAIL_S3_DATAEVENTS_ENABLED
- CLOUDTRAIL_SECURITY_TRAIL_ENABLED
- CLOUDWATCH_ALARM_ACTION_CHECK
- CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK
- CLOUDWATCH_ALARM_RESOURCE_CHECK
- CLOUDWATCH_ALARM_SETTINGS_CHECK
- CLOUDWATCH_LOG_GROUP_ENCRYPTED
- CMK_BACKING_KEY_ROTATION_ENABLED
- CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION
- CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK
- CODEBUILD_PROJECT_ENVVAR_ AWSCRED_CHECK
- CODEBUILD_PROJECT_LOGGING_ENABLED
- CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED
- CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK
- CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED
- CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED
- CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED

Palabras clave de reglas AWS Config administradas compatibles

- CODEPIPELINE_DEPLOYMENT_COUNT_CHECK
- CODEPIPELINE_REGION_FANOUT_CHECK
- CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED
- CW_LOGGROUP_RETENTION_PERIOD_CHECK
- DAX_ENCRYPTION_ENABLED
- DB_INSTANCE_BACKUP_ENABLED
- DESIRED_INSTANCE_TENANCY
- DESIRED_INSTANCE_TYPE
- DMS_REPLICATION_NO_PUBLIC
- DYNAMODB_AUTOSCALING_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_PITR_ENABLED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- DYNAMODB_TABLE_ENCRYPTED_KMS
- DYNAMODB_TABLE_ENCRYPTION_ENABLED
- DYNAMODB_THROUGHPUT_LIMIT_CHECK
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_OPTIMIZED_INSTANCE
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK
- EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL
- EC2_EBS_ENCRYPTION_BY_DEFAULT
- EC2_IMDSV2_CHECK
- EC2_INSTANCE_DETAILED_MONITORING_ENABLED
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_INSTANCE_MULTIPLE_ENI_CHECK
- EC2_INSTANCE_NO_PUBLIC_IP

Palabras clave de reglas AWS Config administradas compatibles

- EC2_INSTANCE_PROFILE_ATTACHED
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED
- EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED
- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED
- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_PLATFORM_CHECK
- EC2_NO_AMAZON_KEY_PAIR
- EC2_PARAVIRTUAL_INSTANCE_CHECK
- EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI
- EC2_SECURITY_GROUP_ADJUNTACHED_TO_ENI_PERIODIC
- EC2_STOPPED_INSTANCE
- EC2_TOKEN_HOP_LIMIT_CHECK
- EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED
- EC2_VOLUME_INUSE_CHECK
- ECR_PRIVATE_IMAGE_SCANNING_ENABLED
- ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED
- ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED
- ECS_ _HABILITADO AWSVPC_NETWORKING
- ECS_CONTAINER_INSIGHTS_ENABLED
- ECS_CONTAINERS_NONPRIVILEGED
- ECS_CONTAINERS_READONLY_ACCESS
- ECS_FARGATE_LATEST_PLATFORM_VERSION
- ECS_NO_ENVIRONMENT_SECRETS
- ECS_TASK_DEFINITION_LOG_CONFIGURATION
- ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT

Palabras clave de reglas AWS Config administradas compatibles

- ECS_TASK_DEFINITION_NONROOT_USER
- ECS_TASK_DEFINITION_PID_MODE_CHECK
- ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK
- EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY
- EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY
- EFS_ENCRYPTED_CHECK
- EFS_IN_BACKUP_PLAN
- EFS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EIP_ATTACHED
- EKS_CLUSTER_LOGGING_ENABLED
- EKS_CLUSTER_OLDEST_SUPPORTED_VERSION
- EKS_CLUSTER_SUPPORTED_VERSION
- EKS_ENDPOINT_NO_PUBLIC_ACCESS
- EKS_SECRETS_ENCRYPTED
- ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH
- ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED
- ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK
- ELASTICACHE_RBAC_AUTH_ENABLED
- ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK
- ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED
- ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST
- ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT
- ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED
- ELASTICACHE_SUBNET_GROUP_CHECK
- ELASTICACHE_SUPPORTED_ENGINE_VERSION
- ELASTICSEARCH_ENCRYPTED_AT_REST
- ELASTICSEARCH_IN_VPC_ONLY
- ELASTICSEARCH_REGISTRA_TO_CLOUDWATCH

Palabras clave de reglas AWS Config administradas compatibles

- ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- ELB_ACM_CERTIFICATE_REQUIRED
- ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK
- ELB_DELETION_PROTECTION_ENABLED
- ELB_LOGGING_ENABLED
- ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK
- ELB_TLS_HTTPS_LISTENERS_ONLY
- ELBV2_ACM_CERTIFICATE_REQUIRED
- ELBV2_MULTIPLE_AZ
- EMR_KERBEROS_ENABLED
- EMR_MASTER_NO_PUBLIC_IP
- ENCRYPTED_VOLUMES
- FMS_SHIELD_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK
- FSX_LAST_BACKUP_RECOVERY_POINT_CREATED
- FSX_RESOURCES_PROTECTED_POR_BACKUP_PLAN
- GUARDDUTY_ENABLED_CENTRALIZED
- GUARDDUTY_NON_ARCHIVED_FINDINGS
- IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS
- IAM_GROUP_HAS_USERS_CHECK
- IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS
- IAM_NO_INLINE_POLICY_CHECK
- IAM_PASSWORD_POLICY
- IAM_POLICY_BLACKLISTED_CHECK
- IAM_POLICY_IN_USE
- IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS
- IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS

Palabras clave de reglas AWS Config administradas compatibles

- IAM_ROLE_MANAGED_POLICY_CHECK
- IAM_ROOT_ACCESS_KEY_CHECK
- IAM_USER_GROUP_MEMBERSHIP_CHECK
- IAM_USER_MFA_ENABLED
- IAM_USER_NO_POLICIES_CHECK
- IAM_USER_UNUSED_CREDENTIALS_CHECK
- INCOMING_SSH_DISABLED
- INSTANCES_IN_VPC
- KINESIS_STREAM_ENCRYPTED
- INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY
- KMS_CMK_NOT_SCHEDULED_FOR_DELETION
- LAMBDA_CONCURRENCY_CHECK
- LAMBDA_DLQ_CHECK
- LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED
- LAMBDA_FUNCTION_SETTINGS_CHECK
- LAMBDA_INSIDE_VPC
- LAMBDA_VPC_MULTI_AZ_CHECK
- MACIE_STATUS_CHECK
- MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS
- MQ_AUTOMATIC_VERSION_MINOR_UPGRADE_ENABLED
- MQ_CLOUDWATCH_AUDIT_LOGGING_HABILITADO
- MQ_NO_PUBLIC_ACCESS
- MULTI_REGION_CLOUD_TRAIL_ENABLED
- NACL_NO_UNRESTRICTED_SSH_RDP
- NETFW_LOGGING_ENABLED
- NETFW_MULTI_AZ_ENABLED
- NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS
- NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS
- NETFW_POLICY_RULE_GROUP_ASSOCIATED

Palabras clave de reglas AWS Config administradas compatibles

- NETFW_STATELESS_RULE_GROUP_NOT_EMPTY
- NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- NO_UNRESTRICTED_ROUTE_TO_IGW
- OPENSEARCH_ACCESS_CONTROL_ENABLED
- OPENSEARCH_AUDIT_LOGGING_ENABLED
- OPENSEARCH_DATA_NODE_FAULT_TOLERANCE
- OPENSEARCH_ENCRYPTED_AT_REST
- OPENSEARCH_HTTPS_REQUIRED
- OPENSEARCH_IN_VPC_ONLY
- OPENSEARCH_LOGS_TO_CLOUDWATCH
- OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- RDS_AUTOMATIC_VERSION_MINOR_UPGRADE_ENABLED
- RDS_CLUSTER_DEFAULT_ADMIN_CHECK
- RDS_CLUSTER_DELETION_PROTECTION_ENABLED
- RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED
- RDS_CLUSTER_MULTI_AZ_ENABLED
- RDS_DB_SECURITY_GROUP_NOT_ALLOWED
- RDS_ENHANCED_MONITORING_ENABLED
- RDS_IN_BACKUP_PLAN
- RDS_INSTANCE_DEFAULT_ADMIN_CHECK
- RDS_INSTANCE_DELETION_PROTECTION_ENABLED
- RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED
- RDS_INSTANCE_PUBLIC_ACCESS_CHECK
- RDS_LAST_BACKUP_RECOVERY_POINT_CREATED
- RDS_LOGGING_ENABLED
- RDS_MULTI_AZ_SUPPORT
- RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- RDS_SNAPSHOT_ENCRYPTED
- RDS_SNAPSHOTS_PUBLIC_PROHIBITED

Palabras clave de reglas AWS Config administradas compatibles

- RDS_STORAGE_ENCRYPTED
- REDSHIFT_BACKUP_ENABLED
- REDSHIFT_REQUIRE_TLS_SSL
- REDSHIFT_CLUSTER_CONFIGURATION_CHECK
- REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK
- REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK
- REDSHIFT_AUDIT_LOGGING_ENABLED
- REDSHIFT_CLUSTER_KMS_ENABLED
- REDSHIFT_DEFAULT_ADMIN_CHECK
- REDSHIFT_DEFAULT_DB_NAME_CHECK
- REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED
- ROOT_ACCOUNT_MFA_ENABLED
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
- S3_BUCKET_ACL_PROHIBITED
- S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED
- S3_BUCKET_DEFAULT_LOCK_ENABLED
- S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED
- S3_BUCKET_LOGGING_ENABLED
- S3_BUCKET_POLICY_GRANTEE_CHECK
- S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE
- S3_BUCKET_PUBLIC_READ_PROHIBITED
- S3_BUCKET_PUBLIC_WRITE_PROHIBITED
- S3_BUCKET_REPLICATION_ENABLED
- S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED
- S3_BUCKET_SSL_REQUESTS_ONLY

Palabras clave de reglas AWS Config administradas compatibles

- S3_BUCKET_VERSIONING_ENABLED
- S3_DEFAULT_ENCRYPTION_KMS
- S3_EVENT_NOTIFICATIONS_ENABLED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_LIFECYCLE_POLICY_CHECK
- S3_RESOURCES_PROTECTED_POR_BACKUP_PLAN
- S3_VERSION_LIFECYCLE_POLICY_CHECK
- SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC
- SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK
- SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS
- SECRETSMANAGER_ROTATION_ENABLED_CHECK
- SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK
- SECRETSMANAGER_SECRET_PERIODIC_ROTATION
- SECRETSMANAGER_SECRET_UNUSED
- SECRETSMANAGER_USING_CMK
- INFORMACIÓN DE LA CUENTA DE SEGURIDAD PROPORCIONADA
- SECURITYHUB_HABILITADO
- SERVICE_VPC_ENDPOINT_ENABLED
- SES_MALWARE_SCANNING_ENABLED
- SHIELD_ADVANCED_ENABLED_AUTORENEW
- SHIELD_DRT_ACCESS
- SNS_ENCRYPTED_KMS
- SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED
- SSM_DOCUMENT_NOT_PUBLIC
- STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Palabras clave de reglas AWS Config administradas compatibles

- SUBRED_AUTO_ASSIGN_PUBLIC_IP_DISABLED
- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VPC_DEFAULT_SECURITY_GROUP_CLOSED
- VPC_FLOW_LOGS_ENABLED
- VPC_NETWORK_ACL_UNUSED_CHECK
- VPC_PEERING_DNS_RESOLUTION_CHECK
- VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS
- VPC_VPN_2_TUNNELS_UP
- WAF_CLASSIC_LOGGING_ENABLED
- WAF_GLOBAL_RULEGROUP_NOT_EMPTY
- WAF_GLOBAL_RULE_NOT_EMPTY
- WAF_GLOBAL_WEBACL_NOT_EMPTY
- WAF_REGIONAL_RULEGROUP_NOT_EMPTY
- WAF_REGIONAL_RULE_NOT_EMPTY
- WAF_REGIONAL_WEBACL_NOT_EMPTY
- WAFV2_LOGGING_ENABLED
- WAFV2_RULEGROUP_NOT_EMPTY
- WAFV2_WEBACL_NOT_EMPTY

Uso de reglas AWS Config personalizadas con Audit Manager

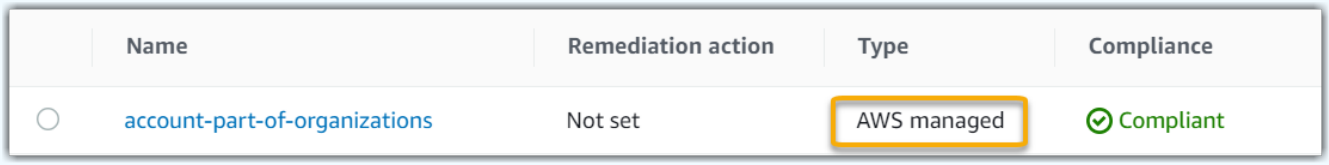
Ahora puede usar reglas AWS Config personalizadas como fuente de datos para los informes de auditoría. Cuando un control tiene una fuente de datos asignada a una AWS Config regla, Audit Manager agrega la evaluación que creó la AWS Config regla.

Las reglas personalizadas que puede utilizar dependen de la forma con la Cuenta de AWS que inicie sesión en Audit Manager. Si puede acceder a una regla personalizada en AWS Config, puede utilizarla como mapeo de fuentes de datos en Audit Manager.

- Para uso individual Cuentas de AWS: puede usar cualquiera de las reglas personalizadas que creó con su cuenta.

- Para las cuentas que forman parte de una organización: también puedes usar cualquiera de sus reglas personalizadas de nivel miembro. O bien, puede usar cualquiera de las reglas personalizadas a nivel de organización que estén disponibles en AWS Config.

Para obtener instrucciones sobre cómo crear un control que utilice reglas personalizadas como origen de datos, consulte Crear un nuevo control desde cero y Personalizar un control existente.

> **Tip**
>
> Tenga en cuenta que las reglas gestionadas no se muestran en la lista desplegable de reglas personalizadas de Audit Manager.
> Si desea comprobar si una AWS Config regla es una regla administrada o una regla personalizada, puede hacerlo mediante la AWS Config consola. En el menú de navegación de la izquierda, seleccione Reglas y busque la regla en la tabla. Si es una regla administrada, la columna Tipo muestra la regla AWS administrada.
>
> 
>
>
> Para mapear una regla administrada como origen de datos, puede buscar la palabra clave del identificador de regla administrada en Audit Manager en la lista desplegable de reglas administradas. Para obtener más información, consulta la sección de resolución de problemas de la guía.

Tras mapear sus reglas personalizadas como un origen de datos para un control, puede asociar ese control a un marco personalizado en Audit Manager. Para obtener instrucciones sobre cómo crear un marco personalizado que utilice su control personalizado, consulte Crear un marco nuevo desde cero y Personalizar un marco existente. Para obtener instrucciones sobre cómo añadir el control a un marco personalizado existente, consulte Editar un marco existente.

Para obtener información sobre cómo crear una regla personalizada en AWS Config, consulte Desarrollo de una regla personalizada AWS Configen la Guía paraAWS Config desarrolladores.

Solución de problemas AWS Config de integración con Audit Manager

Para encontrar respuestas a preguntas y problemas comunes, consulte la AWS Config integración en la sección de solución de problemas de esta guía.

AWS Security Hub controles compatibles con AWS Audit Manager

Audit Manager le permite informar de los resultados de las comprobaciones de conformidad directamente desde Security Hub. Para ello, especifique uno o más controles de Security Hub como mapeo de orígenes de datos al configurar un control personalizado en Audit Manager.

> **Note**
>
> - Audit Manager no recopila pruebas de AWS Config las reglas vinculadas a servicios que crea Security Hub. Para obtener más información, consulta la sección de resolución de problemas de la guía.
> - El 9 de noviembre de 2022, Security Hub lanzó controles de seguridad automatizados alineados con los requisitos de la versión 1.4.0 de AWS Foundations Benchmark del Center for Internet Security (CIS), niveles 1 y 2 (CIS v1.4.0). En Security Hub, se admite el estándar CIS v1.4.0, además del estándar CIS v1.2.0.

Temas

Uso de los controles de Security Hub con Audit Manager

> **Tip**
>
> Le recomendamos que active la configuración de hallazgos de control consolidados en Security Hub si aún no está activada. Si habilitas Security Hub el 23 de febrero de 2003 o después, esta configuración está activada de forma predeterminada.

Cuando las conclusiones consolidadas están habilitadas, Security Hub genera un resultado único para cada control de seguridad (incluso cuando la misma comprobación se aplica a varios estándares). Cada resultado de Security Hub se recopila como una evaluación de recursos única en Audit Manager. En consecuencia, los resultados consolidados revelan una disminución del total de evaluaciones de recursos únicos que Audit Manager realiza para los resultados de Security Hub. Por esta razón, el uso de hallazgos consolidados puede resultar en una reducción de los costos de uso

de Audit Manager a menudo sin sacrificar la calidad y la disponibilidad de las pruebas. Para obtener más información sobre los precios, consulte Precios deAWS Audit Manager.

Ejemplos de pruebas cuando se activa o desactiva la obtención de resultados consolidados

Los siguientes ejemplos muestran una comparación de la forma en que Audit Manager recopila y presenta las pruebas en función de la configuración de Security Hub.

When consolidated findings is turned on

Supongamos que ha activado los tres estándares de seguridad siguientes en Security Hub: AWS FSBP, PCI DSS y CIS Benchmark v1.2.0.

- Estos tres estándares utilizan el mismo control (IAM.4) con la misma regla subyacente (-check). AWS Config iam-root-access-key
- Como la configuración de resultados de control consolidados está activada, Security Hub genera una única búsqueda para este control.
- Security Hub envía el resultado consolidado a Audit Manager para este control.
- El resultado consolidado cuenta como una evaluación de recursos única en Audit Manager. Como resultado, se añade una sola prueba a su evaluación.

A continuación, se muestra un ejemplo de cómo podría verse esa prueba:


```
{
    "SchemaVersion": "2018-10-08",
    "Id": "arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109",
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/securityhub",
    "ProductName": "Security Hub",
    "CompanyName": "AWS",
    "Region": "us-west-2",
    "GeneratorId": "security-control/IAM.4",
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "FirstObservedAt": "2023-10-25T11:32:24.861Z",
    "LastObservedAt": "2023-11-02T11:59:19.546Z",
    "CreatedAt": "2023-10-25T11:32:24.861Z",
    "UpdatedAt": "2023-11-02T11:59:15.127Z",
```

```
    "Severity": {
        "Label": "INFORMATIONAL",
        "Normalized": 0,
        "Original": "INFORMATIONAL"
    },
    "Title": "IAM root user access key should not exist",
    "Description": "This AWS control checks whether the root user access key is
 available.",
    "Remediation": {
        "Recommendation": {
            "Text": "For information on how to correct this issue, consult the AWS
 Security Hub controls documentation.",
            "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
        }
    },
    "ProductFields": {
        "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
check-000270f5",
        "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
        "aws/securityhub/ProductName": "Security Hub",
        "aws/securityhub/CompanyName": "AWS",
        "Resources:0/Id": "arn:aws:iam::111122223333:root",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/aws/
securityhub/arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109"
    },
    "Resources": [{
        "Type": "AwsAccount",
        "Id": "AWS::::Account:111122223333",
        "Partition": "aws",
        "Region": "us-west-2"
    }],
    "Compliance": {
        "Status": "PASSED",
        "RelatedRequirements": [
            "CIS AWS Foundations Benchmark v1.2.0/1.12"
        ],
        "SecurityControlId": "IAM.4",
        "AssociatedStandards": [{
                "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
            },
            {
```

```
                "StandardsId": "standards/aws-foundational-security-best-practices/
v/1.0.0"
            }
        ]
    },
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "RESOLVED"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "INFORMATIONAL"
        },
        "Types": [
            "Software and Configuration Checks/Industry and Regulatory Standards"
        ]
    },
    "ProcessedAt": "2023-11-02T11:59:20.980Z"
}
```

When consolidated findings is turned off

Supongamos que ha activado los tres estándares de seguridad siguientes en Security Hub: AWS FSBP, PCI DSS y CIS Benchmark v1.2.0.

- Estos tres estándares utilizan el mismo control (IAM.4) con la misma regla subyacente (-check). AWS Config iam-root-access-key
- Como la configuración de resultados consolidados está desactivada, Security Hub genera un hallazgo independiente por cada control de seguridad para cada estándar habilitado (en este caso, tres hallazgos).
- Security Hub envía tres conclusiones independientes específicas de la norma a Audit Manager para este control.
- Los tres resultados cuentan como tres evaluaciones de recursos únicas en Audit Manager. Por este motivo, se agregarán tres pruebas independientes a la evaluación.

A continuación, se muestra un ejemplo de cómo podría verse esa prueba. Tenga en cuenta que en este ejemplo, cada una de las tres cargas útiles siguientes tiene el mismo ID de control de seguridad (*SecurityControlId":"IAM.4"*). Por eso, el control de evaluación que recopila

estas pruebas en Audit Manager (IAM.4) recibe tres pruebas distintas cuando Security Hub obtiene los siguientes resultados.

Prueba a favor de la IAM.4 (FSBP)


```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/b5e68d5d-43c3-46c8-902d-51cb0d4da568"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"aws-foundational-security-best-practices/v/1.0.0/IAM.4",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
AWS-Foundational-Security-Best-Practices"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.848Z",
           "LastObservedAt":"2023-11-01T14:12:04.106Z",
           "CreatedAt":"2020-10-05T19:18:47.848Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
              "Product":0,
              "Label":"INFORMATIONAL",
              "Normalized":0,
              "Original":"INFORMATIONAL"
```

```
            },
            "Title":"IAM.4 IAM root user access key should not exist",
            "Description":"This AWS control checks whether the root user access key
 is available.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsArn":"arn:aws:securityhub:::standards/aws-foundational-
security-best-practices/v/1.0.0",
               "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0",
               "ControlId":"IAM.4",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/aws-foundational-security-best-practices/v/1.0.0/IAM.4",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
               "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d"
            },
            "Resources":[
               {
                  "Type":"AwsAccount",
                  "Id":"AWS::::Account:111122223333",
                  "Partition":"aws",
                  "Region":"us-west-2"
               }
            ],
            "Compliance":{
               "Status":"PASSED",
               "SecurityControlId":"IAM.4",
```

```
            "AssociatedStandards":[
               {
                  "StandardsId":"standards/aws-foundational-security-best-
practices/v/1.0.0"
               }
            ]
         },
         "WorkflowState":"NEW",
         "Workflow":{
            "Status":"RESOLVED"
         },
         "RecordState":"ACTIVE",
         "FindingProviderFields":{
            "Severity":{
               "Label":"INFORMATIONAL",
               "Original":"INFORMATIONAL"
            },
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory
 Standards/AWS-Foundational-Security-Best-Practices"
            ]
         },
         "ProcessedAt":"2023-11-01T14:12:07.395Z"
      }
   ]
  }
}
```

Prueba a favor de la IAM.4 (CIS 1.2)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
```

```
    "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0/rule/1.12",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
CIS AWS Foundations Benchmark"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.775Z",
           "LastObservedAt":"2023-11-01T14:12:07.989Z",
           "CreatedAt":"2020-10-05T19:18:47.775Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
              "Product":0,
              "Label":"INFORMATIONAL",
              "Normalized":0,
              "Original":"INFORMATIONAL"
           },
           "Title":"1.12 Ensure no root user access key exists",
           "Description":"The root user is the most privileged user in an AWS
 account. AWS Access Keys provide programmatic access to a given AWS account. It is
 recommended that all access keys associated with the root user be removed.",
           "Remediation":{
              "Recommendation":{
                 "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                 "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
              }
           },
           "ProductFields":{
```

```
              "StandardsGuideArn":"arn:aws:securityhub:::ruleset/cis-aws-
foundations-benchmark/v/1.2.0",
              "StandardsGuideSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/cis-aws-foundations-benchmark/v/1.2.0",
              "RuleId":"1.12",
              "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
              "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
              "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
              "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/cis-aws-foundations-benchmark/v/1.2.0/1.12",
              "aws/securityhub/ProductName":"Security Hub",
              "aws/securityhub/CompanyName":"AWS",
              "Resources:0/Id":"arn:aws:iam::111122223333:root",
              "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
           },
           "Resources":[
              {
                 "Type":"AwsAccount",
                 "Id":"AWS::::Account:111122223333",
                 "Partition":"aws",
                 "Region":"us-west-2"
              }
           ],
           "Compliance":{
              "Status":"PASSED",
              "SecurityControlId":"IAM.4",
              "AssociatedStandards":[
                 {
                    "StandardsId":"ruleset/cis-aws-foundations-benchmark/v/1.2.0"
                 }
              ]
           },
           "WorkflowState":"NEW",
           "Workflow":{
              "Status":"RESOLVED"
           },
           "RecordState":"ACTIVE",
           "FindingProviderFields":{
              "Severity":{
                 "Label":"INFORMATIONAL",
```

```
                "Original":"INFORMATIONAL"
             },
             "Types":[
                "Software and Configuration Checks/Industry and Regulatory
 Standards/CIS AWS Foundations Benchmark"
             ]
          },
          "ProcessedAt":"2023-11-01T14:12:13.436Z"
       }
    ]
  }
}
```

Prueba a favor del PCI.IAM.1 (PCI DSS)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"pci-dss/v/3.2.1/PCI.IAM.1",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
PCI-DSS"
```

```
            ],
            "FirstObservedAt":"2020-10-05T19:18:47.788Z",
            "LastObservedAt":"2023-11-01T14:12:02.413Z",
            "CreatedAt":"2020-10-05T19:18:47.788Z",
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"PCI.IAM.1 IAM root user access key should not exist",
            "Description":"This AWS control checks whether the root user access key
 is available.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsArn":"arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
               "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/pci-dss/v/3.2.1",
               "ControlId":"PCI.IAM.1",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/pci-dss/v/3.2.1/PCI.IAM.1",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
               "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b"
            },
            "Resources":[
               {
                  "Type":"AwsAccount",
```

```
                "Id":"AWS::::Account:111122223333",
                "Partition":"aws",
                "Region":"us-west-2"
             }
          ],
          "Compliance":{
             "Status":"PASSED",
             "RelatedRequirements":[
                "PCI DSS 2.1",
                "PCI DSS 2.2",
                "PCI DSS 7.2.1"
             ],
             "SecurityControlId":"IAM.4",
             "AssociatedStandards":[
                {
                   "StandardsId":"standards/pci-dss/v/3.2.1"
                }
             ]
          },
          "WorkflowState":"NEW",
          "Workflow":{
             "Status":"RESOLVED"
          },
          "RecordState":"ACTIVE",
          "FindingProviderFields":{
             "Severity":{
                "Label":"INFORMATIONAL",
                "Original":"INFORMATIONAL"
             },
             "Types":[
                "Software and Configuration Checks/Industry and Regulatory
 Standards/PCI-DSS"
             ]
          },
          "ProcessedAt":"2023-11-01T14:12:05.950Z"
       }
    ]
  }
}
```

Controles de Security Hub compatibles

Audit Manager admite actualmente los siguientes controles de Security Hub. Puede utilizar cualquiera de las siguientes palabras clave de identificación de control específicas del estándar al configurar un origen de datos para un control personalizado.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
CIS v1.2.0	1.2	IAM.5
CIS v1.2.0	1.3	IAM.8
CIS v1.2.0	1.4	IAM.3
CIS v1.2.0	1.5	IAM.11
CIS v1.2.0	1.6	IAM.12
CIS v1.2.0	1.7	IAM.13
CIS v1.2.0	1.8	IAM.14
CIS v1.2.0	1.9	IAM.15
CIS v1.2.0	1.10	IAM.16
CIS v1.2.0	1.11	IAM.17
CIS v1.2.0	1.12	IAM.4
CIS v1.2.0	1.13	IAM.9
CIS v1.2.0	1.14	IAM.6
CIS v1.2.0	1.16	IAM.2

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
CIS v1.2.0	1.20	IAM.18
CIS v1.2.0	1.22	IAM.1
CIS v1.2.0	2.1	CloudTrail1.
CIS v1.2.0	2.2	CloudTrail.4.
CIS v1.2.0	2.3	CloudTrail6.
CIS v1.2.0	2.4	CloudTrail5.
CIS v1.2.0	2,5	Config.1
CIS v1.2.0	2.6	CloudTrail.7.
CIS v1.2.0	2.7	CloudTrail2.
CIS v1.2.0	2.8	KMS.4
CIS v1.2.0	2.9	EC2.6
CIS v1.2.0	3.1	CloudWatch2.
CIS v1.2.0	3.2	CloudWatch3.
CIS v1.2.0	3.3	CloudWatch1.
CIS v1.2.0	3.4	CloudWatch.4.
CIS v1.2.0	3.5	CloudWatch5.
CIS v1.2.0	3.6	CloudWatch6.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
CIS v1.2.0	3.7	CloudWatch.7.
CIS v1.2.0	3.8	CloudWatch.8.
CIS v1.2.0	3.9	CloudWatch.9.
CIS v1.2.0	3.10	CloudWatch.10
CIS v1.2.0	3.11	CloudWatch.11
CIS v1.2.0	3.12	CloudWatch.12
CIS v1.2.0	3.13	CloudWatch.13
CIS v1.2.0	3.14	CloudWatch.14
CIS v1.2.0	4.1	EC2.13
CIS v1.2.0	4.2	EC2.14
CIS v1.2.0	4.3	EC2.2
PCI DSS	PCI. AutoScaling1.	AutoScaling1.
PCI DSS	PCI. CloudTrail1.	CloudTrail1.
PCI DSS	PCI. CloudTrail2.	CloudTrail2.
PCI DSS	PCI. CloudTrail3.	CloudTrail3.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
PCI DSS	PCI. CloudTrail4.	CloudTrail.4.
PCI DSS	PCI. CodeBuild1.	CodeBuild1.
PCI DSS	PCI. CodeBuild2.	CodeBuild2.
PCI DSS	PCI.config.1	Config.1
PCI DSS	PCI.CW.1	CloudWatch1.
PCI DSS	PCI.DMS.1	DMS.1
PCI DSS	PCI.EC2.1	EC2.1
PCI DSS	PCI.EC2.2	EC2.2
PCI DSS	PCI.EC2.3	EC2.3
PCI DSS	PCI.EC2.4	EC2.12
PCI DSS	PCI.EC2.5	EC2.13
PCI DSS	PCI.EC2.6	EC2.6
PCI DSS	PCI.ELB v2.1	ELB.1
PCI DSS	PCI.ES.1	ES.1
PCI DSS	PCI.ES.2	ES.2

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
PCI DSS	PCI. GuardDuty 1.	GuardDuty1.
PCI DSS	PCI.IAM.1	IAM.1
PCI DSS	PCI.IAM.2	IAM.2
PCI DSS	PCI.IAM.3	IAM.3
PCI DSS	PCI.IAM.4	IAM.4
PCI DSS	PCI.IAM.5	IAM.9
PCI DSS	PCI.IAM.6	IAM.6
PCI DSS	PCI.IAM.7	PCI.IAM.7
PCI DSS	PCI.IAM.8	PCI.IAM8.
PCI DSS	PCI.KMS.1	PCI.KMS.4
PCI DSS	PCI.Lambda.1	Lambda.1
PCI DSS	PCI. Lambda.2	Lambda.3
PCI DSS	PCI.OpenSearch.1	Opensearch.1
PCI DSS	PCI.OpenSearch.2	Opensearch.2
PCI DSS	PCI.RDS.1	RDS.1

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
PCI DSS	PCI.RDS.2	RDS.2
PCI DSS	PCI. Redshift. 1	Redshift.1
PCI DSS	PCIS.3.1	S3.1
PCI DSS	PCI.S3.2	S3.2
PCI DSS	PCI.S3.3	S3.3
PCI DSS	PCI.S3.4	S3.4
PCI DSS	PCI.S3.5	S3.5
PCI DSS	PCI.S3.6	S3.1
PCI DSS	PCI. SageMaker 1.	SageMaker1.
PCI DSS	PCI.SSM.1	SSM.1
PCI DSS	PCI.SSM.2	SSM.2
PCI DSS	PCI.SSM.3	SSM.3
AWS Mejores prácticas de seguridad fundamentales	Account.1	Account.1
AWS Mejores prácticas fundamentales de seguridad	Account.2	Account.2
AWS Mejores prácticas fundamentales de seguridad	ACM.1	ACM.1

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	ACM.2	ACM.2
AWS Mejores prácticas fundamentales de seguridad	APIGateway.1	APIGateway.1
AWS Mejores prácticas fundamentales de seguridad	APIGateway.2	APIGateway.2
AWS Mejores prácticas fundamentales de seguridad	APIGateway.3	APIGateway.3
AWS Mejores prácticas fundamentales de seguridad	APIGateway.4	APIGateway.4
AWS Mejores prácticas fundamentales de seguridad	APIGateway.5	APIGateway.5
AWS Mejores prácticas fundamentales de seguridad	APIGateway.8	APIGateway.8
AWS Mejores prácticas fundamentales de seguridad	APIGateway.9	APIGateway.9
AWS Mejores prácticas fundamentales de seguridad	AppSync2.	AppSync2.
AWS Mejores prácticas de seguridad fundamentales	AppSync5.	AppSync5.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	Athena.1	Athena.1
AWS Mejores prácticas fundamentales de seguridad	AutoScaling1.	AutoScaling1.
AWS Mejores prácticas de seguridad fundamentales	AutoScaling2.	AutoScaling2.
AWS Mejores prácticas de seguridad fundamentales	AutoScaling3.	AutoScaling3.
AWS Mejores prácticas de seguridad fundamentales	AutoScaling4.	AutoScaling.4.
AWS Mejores prácticas fundamentales de seguridad	Autoscaling.5	Autoscaling.5
AWS Mejores prácticas fundamentales de seguridad	AutoScaling6.	AutoScaling6.
AWS Mejores prácticas fundamentales de seguridad	AutoScaling9.	AutoScaling.9.
AWS Mejores prácticas fundamentales de seguridad	Backup.1	Backup.1
AWS Mejores prácticas fundamentales de seguridad	CloudFormation1.	CloudFormation1.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas de seguridad fundamentales	CloudFront1.	CloudFront1.
AWS Mejores prácticas de seguridad fundamentales	CloudFront2.	CloudFront2.
AWS Mejores prácticas de seguridad fundamentales	CloudFront3.	CloudFront3.
AWS Mejores prácticas de seguridad fundamentales	CloudFront4.	CloudFront.4.
AWS Mejores prácticas fundamentales de seguridad	CloudFront5.	CloudFront5.
AWS Mejores prácticas fundamentales de seguridad	CloudFront6.	CloudFront6.
AWS Mejores prácticas fundamentales de seguridad	CloudFront7.	CloudFront7.
AWS Mejores prácticas fundamentales de seguridad	CloudFront8.	CloudFront.8.
AWS Mejores prácticas fundamentales de seguridad	CloudFront9.	CloudFront.9.
AWS Mejores prácticas fundamentales de seguridad	CloudFront.10	CloudFront.10

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	CloudFront1.2	CloudFront.12
AWS Mejores prácticas fundamentales de seguridad	CloudFront1.3	CloudFront.13
AWS Mejores prácticas fundamentales de seguridad	CloudTrail1.	CloudTrail1.
AWS Mejores prácticas de seguridad fundamentales	CloudTrail2.	CloudTrail2.
AWS Mejores prácticas de seguridad fundamentales	CloudTrail3.	CloudTrail3.
AWS Mejores prácticas de seguridad fundamentales	CloudTrail4.	CloudTrail.4.
AWS Mejores prácticas fundamentales de seguridad	CloudTrail5.	CloudTrail5.
AWS Mejores prácticas fundamentales de seguridad	CloudTrail6.	CloudTrail6.
AWS Mejores prácticas fundamentales de seguridad	CloudTrail7.	CloudTrail7.
AWS Mejores prácticas fundamentales de seguridad	CloudWatch1.	CloudWatch1.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas de seguridad fundamentales	CloudWatch2.	CloudWatch2.
AWS Mejores prácticas de seguridad fundamentales	CloudWatch3.	CloudWatch3.
AWS Mejores prácticas de seguridad fundamentales	CloudWatch4.	CloudWatch.4.
AWS Mejores prácticas fundamentales de seguridad	CloudWatch5.	CloudWatch5.
AWS Mejores prácticas fundamentales de seguridad	CloudWatch6.	CloudWatch6.
AWS Mejores prácticas fundamentales de seguridad	CloudWatch7.	CloudWatch7.
AWS Mejores prácticas fundamentales de seguridad	CloudWatch8.	CloudWatch.8.
AWS Mejores prácticas fundamentales de seguridad	CloudWatch9.	CloudWatch.9.
AWS Mejores prácticas fundamentales de seguridad	CloudWatch.10	CloudWatch.10
AWS Mejores prácticas fundamentales de seguridad	CloudWatch1.1	CloudWatch.11

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	CloudWatch1.2	CloudWatch.12
AWS Mejores prácticas fundamentales de seguridad	CloudWatch1.3	CloudWatch.13
AWS Mejores prácticas fundamentales de seguridad	CloudWatch1.4	CloudWatch.14
AWS Mejores prácticas fundamentales de seguridad	CloudWatch1.5	CloudWatch.15
AWS Mejores prácticas fundamentales de seguridad	CloudWatch1.6	CloudWatch.16
AWS Mejores prácticas fundamentales de seguridad	CloudWatch1.7	CloudWatch.17
AWS Mejores prácticas fundamentales de seguridad	CodeBuild1.	CodeBuild1.
AWS Mejores prácticas de seguridad fundamentales	CodeBuild2.	CodeBuild2.
AWS Mejores prácticas de seguridad fundamentales	CodeBuild3.	CodeBuild3.
AWS Mejores prácticas de seguridad fundamentales	CodeBuild4.	CodeBuild.4.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	CodeBuild5.	CodeBuild5.
AWS Mejores prácticas fundamentales de seguridad	Config. 1	Config.1
AWS Mejores prácticas fundamentales de seguridad	DMS.1	DMS.1
AWS Mejores prácticas fundamentales de seguridad	DMS.6	DMS.6
AWS Mejores prácticas fundamentales de seguridad	DMS.7	DMS.7
AWS Mejores prácticas fundamentales de seguridad	DMS.8	DMS.8
AWS Mejores prácticas fundamentales de seguridad	DMS.9	DMS.9
AWS Mejores prácticas fundamentales de seguridad	DocumentDB.1	DocumentDB.1
AWS Mejores prácticas fundamentales de seguridad	DocumentDB.2	DocumentDB.2
AWS Mejores prácticas fundamentales de seguridad	DocumentDB.3	DocumentDB.3

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	DocumentDB.4	DocumentDB.4
AWS Mejores prácticas fundamentales de seguridad	DocumentDB.5	DocumentDB.5
AWS Mejores prácticas fundamentales de seguridad	DynamoDB.1	DynamoDB.1
AWS Mejores prácticas fundamentales de seguridad	DynamoDB.2	DynamoDB.2
AWS Mejores prácticas fundamentales de seguridad	DynamoDB.3	DynamoDB.3
AWS Mejores prácticas fundamentales de seguridad	DynamoDB.4	DynamoDB.4
AWS Mejores prácticas fundamentales de seguridad	DynamoDB.6	DynamoDB.6
AWS Mejores prácticas fundamentales de seguridad	EC2.1	EC2.1
AWS Mejores prácticas fundamentales de seguridad	EC2.2	EC2.2
AWS Mejores prácticas fundamentales de seguridad	EC2.3	EC2.3

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	EC2.4	EC2.4
AWS Mejores prácticas fundamentales de seguridad	EC2.6	EC2.6
AWS Mejores prácticas fundamentales de seguridad	EC2.7	EC2.7
AWS Mejores prácticas fundamentales de seguridad	EC2.8	EC2.8
AWS Mejores prácticas fundamentales de seguridad	EC2.9	EC2.9
AWS Mejores prácticas fundamentales de seguridad	EC2.10	EC2.10
AWS Mejores prácticas fundamentales de seguridad	EC2.12	EC2.12
AWS Mejores prácticas fundamentales de seguridad	EC2.13	EC2.13
AWS Mejores prácticas fundamentales de seguridad	EC2.14	EC2.14
AWS Mejores prácticas fundamentales de seguridad	EC2.15	EC2.15

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	EC2.16	EC2.16
AWS Mejores prácticas fundamentales de seguridad	EC2.17	EC2.17
AWS Mejores prácticas fundamentales de seguridad	EC2.18	EC2.18
AWS Mejores prácticas fundamentales de seguridad	EC2.19	EC2.19
AWS Mejores prácticas fundamentales de seguridad	EC2.20	EC2.20
AWS Mejores prácticas fundamentales de seguridad	EC2.21	EC2.21
AWS Mejores prácticas fundamentales de seguridad	EC2.22	EC2.22
AWS Mejores prácticas fundamentales de seguridad	EC 2.23	EC2.23
AWS Mejores prácticas fundamentales de seguridad	EC2.24	EC2.24
AWS Mejores prácticas fundamentales de seguridad	EC2.25	EC2.25

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	EC2.28	EC2.28
AWS Mejores prácticas fundamentales de seguridad	EC2.51	EC2.51
AWS Mejores prácticas fundamentales de seguridad	ECR.1	ECR.1
AWS Mejores prácticas fundamentales de seguridad	ECR.2	ECR.2
AWS Mejores prácticas fundamentales de seguridad	ECR.3	ECR.3
AWS Mejores prácticas fundamentales de seguridad	ECS.1	ECS.1
AWS Mejores prácticas fundamentales de seguridad	ECS.2	ECS.2
AWS Mejores prácticas fundamentales de seguridad	ECS.3	ECS.3
AWS Mejores prácticas fundamentales de seguridad	ECS.4	ECS.4
AWS Mejores prácticas fundamentales de seguridad	ECS.5	ECS.5

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	ECS.8	ECS.8
AWS Mejores prácticas fundamentales de seguridad	ECS.9	ECS.9
AWS Mejores prácticas fundamentales de seguridad	ECS.10	ECS.10
AWS Mejores prácticas fundamentales de seguridad	ECS.12	ECS.12
AWS Mejores prácticas fundamentales de seguridad	EFS.1	EFS.1
AWS Mejores prácticas fundamentales de seguridad	EFS 2	EFS. 2
AWS Mejores prácticas fundamentales de seguridad	EFS 3	EFS.3
AWS Mejores prácticas fundamentales de seguridad	EFS 4	EFS.4
AWS Mejores prácticas fundamentales de seguridad	EKS.1	EKS.1
AWS Mejores prácticas fundamentales de seguridad	EKS.2	EKS.2

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	EKS.8	EKS.8
AWS Mejores prácticas fundamentales de seguridad	ElastiCache1.	ElastiCache1.
AWS Mejores prácticas de seguridad fundamentales	ElastiCache2.	ElastiCache2.
AWS Mejores prácticas de seguridad fundamentales	ElastiCache3.	ElastiCache3.
AWS Mejores prácticas de seguridad fundamentales	ElastiCache4.	ElastiCache.4.
AWS Mejores prácticas fundamentales de seguridad	ElastiCache5.	ElastiCache5.
AWS Mejores prácticas fundamentales de seguridad	ElastiCache6.	ElastiCache6.
AWS Mejores prácticas fundamentales de seguridad	ElastiCache7.	ElastiCache7.
AWS Mejores prácticas fundamentales de seguridad	ElasticBeanstalk1.	ElasticBeanstalk1.
AWS Mejores prácticas de seguridad fundamentales	ElasticBeanstalk2.	ElasticBeanstalk2.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas de seguridad fundamentales	ElasticBeanstalk3.	ElasticBeanstalk3.
AWS Mejores prácticas de seguridad fundamentales	ELB.1	ELB.1
AWS Mejores prácticas fundamentales de seguridad	ELB.2	ELB.2
AWS Mejores prácticas fundamentales de seguridad	ELB.3	ELB.3
AWS Mejores prácticas fundamentales de seguridad	ELB.4	ELB.4
AWS Mejores prácticas fundamentales de seguridad	ELB.5	ELB.5
AWS Mejores prácticas fundamentales de seguridad	ELB.6	ELB.6
AWS Mejores prácticas fundamentales de seguridad	ELB.7	ELB.7
AWS Mejores prácticas fundamentales de seguridad	ELB.8	ELB.8
AWS Mejores prácticas fundamentales de seguridad	ELB.9	ELB.9

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	ELB.10	ELB.10
AWS Mejores prácticas fundamentales de seguridad	ELB.12	ELB.12
AWS Mejores prácticas fundamentales de seguridad	ELB.13	ELB.13
AWS Mejores prácticas fundamentales de seguridad	ELB.14	ELB.14
AWS Mejores prácticas fundamentales de seguridad	ELB.16	ELB.16
AWS Mejores prácticas fundamentales de seguridad	ELBv2.1	ELB.1
AWS Mejores prácticas fundamentales de seguridad	EMR.1	EMR.1
AWS Mejores prácticas fundamentales de seguridad	EMR.2	EMR.2
AWS Mejores prácticas fundamentales de seguridad	ES.1	ES.1
AWS Mejores prácticas fundamentales de seguridad	ES.2	ES.2

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	ES.3	ES.3
AWS Mejores prácticas fundamentales de seguridad	ES.4	ES.4
AWS Mejores prácticas fundamentales de seguridad	ES.5	ES.5
AWS Mejores prácticas fundamentales de seguridad	ES.6	ES.6
AWS Mejores prácticas fundamentales de seguridad	ES.7	ES.7
AWS Mejores prácticas fundamentales de seguridad	ES.8	ES.8
AWS Mejores prácticas fundamentales de seguridad	EventBridge3.	EventBridge3.
AWS Mejores prácticas fundamentales de seguridad	EventBridge4.	EventBridge.4.
AWS Mejores prácticas fundamentales de seguridad	FSx.1	FSx.1
AWS Mejores prácticas fundamentales de seguridad	GuardDuty1.	GuardDuty1.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas de seguridad fundamentales	IAM.1	IAM.1
AWS Mejores prácticas fundamentales de seguridad	IAM.2	IAM.2
AWS Mejores prácticas fundamentales de seguridad	IAM.3	IAM.3
AWS Mejores prácticas fundamentales de seguridad	IAM.4	IAM.4
AWS Mejores prácticas fundamentales de seguridad	IAM.5	IAM.5
AWS Mejores prácticas fundamentales de seguridad	IAM.6	IAM.6
AWS Mejores prácticas fundamentales de seguridad	IAM.7	IAM.7
AWS Mejores prácticas fundamentales de seguridad	IAM.8	IAM.8
AWS Mejores prácticas fundamentales de seguridad	IAM.9	IAM.9
AWS Mejores prácticas fundamentales de seguridad	IAM.10	IAM.10

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	IAM.11	IAM.11
AWS Mejores prácticas fundamentales de seguridad	IAM.12	IAM.12
AWS Mejores prácticas fundamentales de seguridad	IAM.13	IAM.13
AWS Mejores prácticas fundamentales de seguridad	IAM.14	IAM.14
AWS Mejores prácticas fundamentales de seguridad	IAM.15	IAM.15
AWS Mejores prácticas fundamentales de seguridad	IAM.16	IAM.16
AWS Mejores prácticas fundamentales de seguridad	IAM.17	IAM.17
AWS Mejores prácticas fundamentales de seguridad	IAM.18	IAM.18
AWS Mejores prácticas fundamentales de seguridad	IAM.19	IAM.19
AWS Mejores prácticas fundamentales de seguridad	IAM.21	IAM.21

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	IAM.22	IAM.22
AWS Mejores prácticas fundamentales de seguridad	Kinesis.1	Kinesis.1
AWS Mejores prácticas fundamentales de seguridad	KMS.1	KMS.1
AWS Mejores prácticas fundamentales de seguridad	KMS.2	KMS.2
AWS Mejores prácticas fundamentales de seguridad	KMS.3	KMS.3
AWS Mejores prácticas fundamentales de seguridad	KMS.4	KMS.4
AWS Mejores prácticas fundamentales de seguridad	Lambda.1	Lambda.1
AWS Mejores prácticas fundamentales de seguridad	Lambda.2	Lambda.2
AWS Mejores prácticas fundamentales de seguridad	Lambda 3	Lambda 3
AWS Mejores prácticas fundamentales de seguridad	Lambda.5	Lambda.5

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	Macie.1	Macie.1
AWS Mejores prácticas fundamentales de seguridad	MQ.5	MQ.5
AWS Mejores prácticas fundamentales de seguridad	MQ.6	MQ.6
AWS Mejores prácticas fundamentales de seguridad	MSK.1	MSK.1
AWS Mejores prácticas fundamentales de seguridad	MSK.2	MSK.2
AWS Mejores prácticas fundamentales de seguridad	Neptune.1	Neptune.1
AWS Mejores prácticas fundamentales de seguridad	Neptune.2	Neptune.2
AWS Mejores prácticas fundamentales de seguridad	Neptune.3	Neptune.3
AWS Mejores prácticas fundamentales de seguridad	Neptune.4	Neptune.4
AWS Mejores prácticas fundamentales de seguridad	Neptune.5	Neptune.5

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	Neptune.6	Neptune.6
AWS Mejores prácticas fundamentales de seguridad	Neptune.7	Neptune.7
AWS Mejores prácticas fundamentales de seguridad	Neptune.8	Neptune.8
AWS Mejores prácticas fundamentales de seguridad	Neptune.9	Neptune.9
AWS Mejores prácticas fundamentales de seguridad	NetworkFirewall1.	NetworkFirewall1.
AWS Mejores prácticas de seguridad fundamentales	NetworkFirewall2.	NetworkFirewall2.
AWS Mejores prácticas de seguridad fundamentales	NetworkFirewall3.	NetworkFirewall3.
AWS Mejores prácticas de seguridad fundamentales	NetworkFirewall4.	NetworkFirewall.4.
AWS Mejores prácticas fundamentales de seguridad	NetworkFirewall5.	NetworkFirewall5.
AWS Mejores prácticas fundamentales de seguridad	NetworkFirewall6.	NetworkFirewall6.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	NetworkFirewall9.	NetworkFirewall.9.
AWS Mejores prácticas fundamentales de seguridad	Opensearch.1	Opensearch.1
AWS Mejores prácticas fundamentales de seguridad	Opensearch.2	Opensearch.2
AWS Mejores prácticas fundamentales de seguridad	Opensearch.3	Opensearch.3
AWS Mejores prácticas fundamentales de seguridad	Opensearch.4	Opensearch.4
AWS Mejores prácticas fundamentales de seguridad	Opensearch.5	Opensearch.5
AWS Mejores prácticas fundamentales de seguridad	Opensearch.6	Opensearch.6
AWS Mejores prácticas fundamentales de seguridad	Opensearch.7	Opensearch.7
AWS Mejores prácticas fundamentales de seguridad	Opensearch.8	Opensearch.8
AWS Mejores prácticas fundamentales de seguridad	Opensearch.10	Opensearch.10

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	PCA.1	PCA.1
AWS Mejores prácticas fundamentales de seguridad	RDS.1	RDS.1
AWS Mejores prácticas fundamentales de seguridad	RDS.2	RDS.2
AWS Mejores prácticas fundamentales de seguridad	RDS.3	RDS.3
AWS Mejores prácticas fundamentales de seguridad	RED.4	RDS.4
AWS Mejores prácticas fundamentales de seguridad	RDS.5	RDS.5
AWS Mejores prácticas fundamentales de seguridad	RDS.6	RDS.6
AWS Mejores prácticas fundamentales de seguridad	RDS.7	RDS.7
AWS Mejores prácticas fundamentales de seguridad	RDS.8	RDS.8
AWS Mejores prácticas fundamentales de seguridad	RDS.9	RDS.9

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	RDS.10	RDS.10
AWS Mejores prácticas fundamentales de seguridad	RDS.11	RDS.11
AWS Mejores prácticas fundamentales de seguridad	RDS.12	RDS.12
AWS Mejores prácticas fundamentales de seguridad	RDS.13	RDS.13
AWS Mejores prácticas fundamentales de seguridad	RDS.14	RDS.14
AWS Mejores prácticas fundamentales de seguridad	RDS.15	RDS.15
AWS Mejores prácticas fundamentales de seguridad	RDS.16	RDS.16
AWS Mejores prácticas fundamentales de seguridad	RDS.17	RDS.17
AWS Mejores prácticas fundamentales de seguridad	RDS.18	RDS.18
AWS Mejores prácticas fundamentales de seguridad	RDS.19	RDS.19

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	RDS.20	RDS.20
AWS Mejores prácticas fundamentales de seguridad	RDS.21	RDS.21
AWS Mejores prácticas fundamentales de seguridad	RDS.22	RDS.22
AWS Mejores prácticas fundamentales de seguridad	RDS.23	RDS.23
AWS Mejores prácticas fundamentales de seguridad	RDS.24	RDS.24
AWS Mejores prácticas fundamentales de seguridad	RDS.25	RDS.25
AWS Mejores prácticas fundamentales de seguridad	RDS.26	RDS.26
AWS Mejores prácticas fundamentales de seguridad	RDS.27	RDS.27
AWS Mejores prácticas fundamentales de seguridad	RDS.34	RDS.34
AWS Mejores prácticas fundamentales de seguridad	RDS.35	RDS.35

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	Redshift.1	Redshift.1
AWS Mejores prácticas fundamentales de seguridad	Redshift.2	Redshift.2
AWS Mejores prácticas fundamentales de seguridad	Redshift.3	Redshift.3
AWS Mejores prácticas fundamentales de seguridad	Redshift.4	Redshift.4
AWS Mejores prácticas fundamentales de seguridad	Redshift.6	Redshift.6
AWS Mejores prácticas fundamentales de seguridad	Redshift.7	Redshift.7
AWS Mejores prácticas fundamentales de seguridad	Redshift.8	Redshift.8
AWS Mejores prácticas fundamentales de seguridad	Redshift.9	Redshift.9
AWS Mejores prácticas fundamentales de seguridad	Redshift.10	Redshift.10
AWS Mejores prácticas fundamentales de seguridad	Route53.2	Route53.2

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	S3.1	S3.1
AWS Mejores prácticas fundamentales de seguridad	S3.2	S3.2
AWS Mejores prácticas fundamentales de seguridad	S3.3	S3.3
AWS Mejores prácticas fundamentales de seguridad	S3.4	S3.4
AWS Mejores prácticas fundamentales de seguridad	S3.5	S3.5
AWS Mejores prácticas fundamentales de seguridad	S3.6	S3.6
AWS Mejores prácticas fundamentales de seguridad	S3.7	S3.7
AWS Mejores prácticas fundamentales de seguridad	S3.8	S3.8
AWS Mejores prácticas fundamentales de seguridad	S3.9	S3.9
AWS Mejores prácticas fundamentales de seguridad	S3.11	S3.11

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	S3.12	S3.12
AWS Mejores prácticas fundamentales de seguridad	S3.13	S3.13
AWS Mejores prácticas fundamentales de seguridad	S3.14	S3.14
AWS Mejores prácticas fundamentales de seguridad	S3.15	S3.15
AWS Mejores prácticas fundamentales de seguridad	S3.17	S3.17
AWS Mejores prácticas fundamentales de seguridad	S3.19	S3.19
AWS Mejores prácticas fundamentales de seguridad	S3.19	S3.20
AWS Mejores prácticas fundamentales de seguridad	SageMaker1.	SageMaker1.
AWS Mejores prácticas de seguridad fundamentales	SageMaker2.	SageMaker2.
AWS Mejores prácticas de seguridad fundamentales	SageMaker3.	SageMaker3.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas de seguridad fundamentales	SecretsManager1.	SecretsManager1.
AWS Mejores prácticas de seguridad fundamentales	SecretsManager2.	SecretsManager2.
AWS Mejores prácticas de seguridad fundamentales	SecretsManager3.	SecretsManager3.
AWS Mejores prácticas de seguridad fundamentales	SecretsManager4.	SecretsManager.4.
AWS Mejores prácticas fundamentales de seguridad	SNS.1	SNS.1
AWS Mejores prácticas fundamentales de seguridad	SNS.2	SNS.2
AWS Mejores prácticas fundamentales de seguridad	SQS.1	SQS.1
AWS Mejores prácticas fundamentales de seguridad	SSM.1	SSM.1
AWS Mejores prácticas fundamentales de seguridad	SSM.2	SSM.2
AWS Mejores prácticas fundamentales de seguridad	SSM 3	SSM.3

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	SSM 4	SSM.4
AWS Mejores prácticas fundamentales de seguridad	StepFunctions1.	StepFunctions1.
AWS Mejores prácticas de seguridad fundamentales	WAF.1	WAF.1
AWS Mejores prácticas fundamentales de seguridad	WAF.2	WAF.2
AWS Mejores prácticas fundamentales de seguridad	WAF.3	WAF.3
AWS Mejores prácticas fundamentales de seguridad	WAF.4	WAF.4
AWS Mejores prácticas fundamentales de seguridad	WAF.6	WAF.6
AWS Mejores prácticas fundamentales de seguridad	WAF.7	WAF.7
AWS Mejores prácticas fundamentales de seguridad	WAF.8	WAF.8
AWS Mejores prácticas fundamentales de seguridad	WAF.10	WAF.10

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	WAF.11	WAF.11
AWS Mejores prácticas fundamentales de seguridad	WAF.12	WAF.12

Las llamadas a la API son compatibles con AWS Audit Manager

Audit Manager realiza llamadas a la API Servicios de AWS para recopilar una instantánea de los detalles de configuración de sus AWS recursos. Puede especificar estas llamadas a la API como un mapeo de orígenes de datos al configurar un control personalizado en Audit Manager.

Audit Manager realiza una instantánea de la configuración de cada recurso que esté en el ámbito de una llamada a la API y la convierte en prueba. Esto da como resultado una prueba por recurso, en lugar de una prueba por llamada a la API.

Por ejemplo, si la llamada a la API `ec2_DescribeRouteTables` captura instantáneas de la configuración de cinco tablas de rutas, obtendrá cinco pruebas en total para cada llamada a la API. Cada prueba es una instantánea de la configuración de una tabla de enrutamiento individual.

En esta página

Se admiten llamadas a la API para orígenes de datos de control personalizadas

En sus controles personalizados, puede usar cualquiera de las siguientes llamadas a la API como origen de datos. A continuación, Audit Manager puede utilizar estas llamadas a la API para recopilar pruebas sobre su AWS uso.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
acm_ GetAccountConfiguration	Recopila una instantánea de las opciones de configuración de la cuenta asociadas a su Cuenta de AWS.
acm_ ListCertificates	Recupera una lista de los ARN de los certificados y los nombres de dominio.
cloudtrail_ DescribeTrails	Recopila una instantánea de la configuración de uno o más registros asociados a la región actual de su Cuenta de AWS.
cloudwatch_ DescribeAlarms	Recopila una instantánea de la configuración de las alarmas que se utilizan en su Cuenta de AWS.
config_ DescribeConfigRules	Recupera detalles sobre tus reglas. AWS Config
config_ DescribeDeliveryChannels	Recopila una instantánea de la configuración de los canales de entrega en su Cuenta de AWS.
directconnect_ DescribeDirectConnectGateways	Recupera una lista de todas tus puertas de enlace. AWS Direct Connect
directconnect_ DescribeVirtualGateways	Recupera una lista de las puertas de enlace privadas virtuales que son de su Cuenta de AWS.
docdb_ DescribeCertificates	Recopila una lista de certificados para su Cuenta de AWS.
docDB_DescribeDB ClusterParameterGroups	Recopila una lista de descripciones de `DBClusterParameterGroup` para su Cuenta de AWS.
docdb_DescribeDBInstances	Recopila información sobre las instancias de Amazon DynamoDB aprovisionadas para su Cuenta de AWS.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
dynamodb_ DescribeTable	Recopila instantáneas de configuración para las tablas de DynamoDB de su Cuenta de AWS. Cuando utiliza esta API como origen de datos, no necesita proporcionar el nombre de una tabla de DynamoDB específica. En su lugar, Audit Manager utiliza la operación `ListTables` para enumerar todas las tablas. Para cada tabla que aparece en la lista, Audit Manager realiza la operación `DescribeTable` para generar prueba para ese recurso.
dynamodb_ ListBackups	Recupera una lista de las copias de seguridad de DynamoDB que están asociadas a su Cuenta de AWS.
dynamodb_ ListGlobalTables	Recupera una lista de todas las tablas globales que se encuentran actualmente en su Cuenta de AWS.
dynamodb_ ListTables	Recupera una lista de todos los nombres de las tablas que están asociados a su Cuenta de AWS y a su punto de conexión actual.
ec2_ DescribeAddresses	Recopila una instantánea de sus direcciones IP elásticas.
ec2_ DescribeCustomerGateways	Recopila una instantánea de las puertas de enlace de cliente de VPN.
ec2_ DescribeEgressOnlyInternetGateways	Recopila una instantánea de sus puertas de enlace de Internet de solo salida.
ec2_ DescribeFlowLogs	Recopila una instantánea de los registros de flujo.
ec2_ DescribeInstances	Recopila una instantánea de sus instancias.
ec2_ DescribeInternetGateways	Recopila una instantánea de sus puertas de enlace de Internet.
ec2_ DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	Recopile una descripción de las asociaciones entre los grupos de interfaces virtuales y las tablas de enrutamiento de las puertas de enlace locales de su. Cuenta de AWS

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
ec2_ DescribeLocalGateways	Recopila una instantánea de sus puertas de enlace locales.
ec2_ DescribeLocalGatewayVirtualInterfaces	Recopila una instantánea de las interfaces virtuales de su puerta de enlace local.
ec2_ DescribeNatGateways	Recopila una instantánea de sus puertas de enlace NAT.
ec2_ DescribeNetworkAcls	Recopila una instantánea de las ACL de la red.
ec2_ DescribeRouteTables	Recopila una instantánea de sus tablas de enrutamiento.
ec2_ DescribeSecurityGroups	Recopila una instantánea de sus grupos de seguridad.
ec2_ DescribeTransitGateways	Recopila una instantánea de sus puertas de enlace de tránsito.
ec2_ DescribeVolumes	Recopila una instantánea de sus puntos de conexión de VPC.
ec2_ DescribeVpcs	Recopila una instantánea de sus VPC.
ec2_ DescribeVpcEndpoints	Recopila una instantánea de sus puntos de conexión de VPC.
ec2_ DescribeVpcPeeringConnections	Recopila una instantánea de sus conexiones VPN.
ec2_ DescribeVpnConnections	Recopila una instantánea de sus conexiones VPN.
ec2_ DescribeVpnGateways	Recopila una instantánea de sus puertas de enlace privadas virtuales.
ec2_ GetEbsDefaultKmsKeyId	Recopile una instantánea del cifrado EBS predeterminado AWS KMS key para su Cuenta de AWS región actual.
ec2_ GetEbsEncryptionByDefault	Describe si el cifrado EBS está habilitado de forma predeterminada para su Cuenta de AWS en la región actual.
ecs_ DescribeClusters	Recopila una instantánea de los clústeres de ECS.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
eks_ DescribeAddonVersions	Recopila una instantánea de las versiones de los complementos.
dolor elástico_ DescribeCacheClusters	Recopila una instantánea de sus clústeres aprovisionados.
dolor elástico_ DescribeServiceUpdates	Recopila una instantánea de las actualizaciones de los servicios de Amazon ElastiCache.
elasticfilesystem_ DescribeAccessPoints	Recopile una instantánea de los puntos de acceso de Amazon EFS en su Cuenta de AWS.
elasticfilesystem_ DescribeFileSystems	Recopila una instantánea de sus sistemas de archivos de Amazon EFS.
balanceo de carga elástico v2_ DescribeLoadBalancers	Recopile una instantánea de los balanceadores de carga de su. Cuenta de AWS
elasticloadbalancingv2_DescribeSSLPolicies	Recopila una instantánea de las políticas que utiliza para la negociación de SSL.
balanceo de carga elástico v2_ DescribeTargetGroups	Recopila una instantánea de sus grupos de destino de ELB.
elasticmapreduce_ ListSecurityConfigurations	Recupera una lista de las configuraciones de seguridad que tiene visibles en su Cuenta de AWS, junto con sus fechas y horas de creación y sus nombres.
eventos_ ListConnections	Recupera una lista de las EventBridge conexiones de Amazon en tu Cuenta de AWS.
eventos_ ListEventBuses	Obtenga una lista de los autobuses de EventBridge eventos de Amazon que tiene en su Cuenta de AWSpoder, incluidos el autobús de eventos predeterminado, los autobuses de eventos personalizados y los autobuses de eventos asociados.
eventos_ ListEventSources	Recupera una lista de los orígenes de eventos de socios que se han compartido con su Cuenta de AWS.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
eventos_ ListRules	Recupera una lista de tus EventBridge reglas de Amazon.
firehose_ ListDeliveryStreams	Recupera una lista de sus flujos de entrega.
fsx_ DescribeFileSystems	Recopila una instantánea de los sistemas de archivos que le pertenecen a su Cuenta de AWS.
guardiana_ ListDetectors	Obtenga una lista de los recursos `detectorIds` de su GuardDuty detector de Amazon.
iam_ GenerateCredential Report	Genera un informe de credencial para su Cuenta de AWS.
iam_ GetAccountPassword Policy	Recopila una instantánea de la política de contraseñas de su Cuenta de AWS.
iam_ GetAccountSummary	Recopila una instantánea del uso de entidades de IAM y cuotas de IAM en su Cuenta de AWS.
iam_ ListGroupPolicies	Obtenga una lista de las políticas en línea integradas en un grupo de IAM que esté disponible en su. Cuenta de AWS
iam_ ListGroups	Obtenga una lista de los grupos de IAM que están asociados a un prefijo de ruta que esté disponible en su. Cuenta de AWS
iam_ ID ListOpen ConnectPr oviders	Recupera una lista de los objetos del recurso del proveedor OpenID Connect (OIDC) de IAM que están definidos en su Cuenta de AWS.
iam_ ListPolicies	Recupera una lista de todas las políticas administradas que están disponibles en su Cuenta de AWS, incluidas las políticas administradas definidas por su propio cliente y todas las políticas administradas por AWS.
iam_ ListRoles	Obtenga una lista de las funciones de IAM asociadas a un prefijo de ruta que esté disponible en su. Cuenta de AWS

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
iam_ListSAMLProviders	Recupera una lista de los objetos del recurso del proveedor SAML que están definidos en IAM en su Cuenta de AWS.
iam_ ListUsers	Recupere una lista de los usuarios de IAM de su. Cuenta de AWS
ListVirtualiam_ MFA Devices	Recupera una lista de los dispositivos MFA virtuales que están definidos en su Cuenta de AWS.
kafka_ ListClusters	Obtenga una lista de los clústeres de Amazon MSK en su Cuenta de AWS.
kafka_ ListKafkaVersions	Recupera una lista de los objetos de la versión de Apache Kafka en su Cuenta de AWS.
kinesis_ ListStreams	Recupera una lista de sus flujos de datos de Kinesis.
kms_ GetKeyPolicy	Audit Manager utiliza esta API para recopilar una instantánea de las políticas de claves para AWS KMS keys en su Cuenta de AWS. Cuando utilizas esta API como fuente de datos, no necesitas proporcionar el nombre de una específica. AWS KMS keyEn su lugar, Audit Manager utiliza la operación `ListKeys` para enumerar todas las claves de KMS. Por cada clave de KMS que aparece en la lista, Audit Manager realiza la operación `GetKeyPolicy` con el fin de generar prueba para ese recurso.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
kms_ GetKeyRotationStatus	Audit Manager utiliza esta API para recopilar una instantánea de si la rotación automática está AWS KMS keys habilitada para su Cuenta de AWS. Cuando utilizas esta API como fuente de datos, no necesitas proporcionar el nombre de una específica AWS KMS key. En su lugar, Audit Manager utiliza la operación `ListKeys` para enumerar todas las claves de KMS. Por cada clave de KMS que aparece en la lista, Audit Manager realiza la operación `GetKeyRotationStatus` con el fin de generar prueba para ese recurso.
kms_ ListKeys	Recupere una lista de los que están AWS KMS keys en su. Cuenta de AWS
lambda_ ListFunctions	Obtenga una lista de las funciones de Lambda que tenga en su ordenador Cuenta de AWS, con la configuración específica de cada versión de cada una.
rds_DescribeDBClusters	Recopile una instantánea de los clústeres de base de datos Amazon Aurora y los clústeres de base de datos Multi-AZ existentes en su Cuenta de AWS.
rds_DescribeDBInstances	Recopila una instantánea de las instancias de RDS aprovisio nadas en su Cuenta de AWS.
redshift_ DescribeClusters	Recopila una instantánea de los clústeres de Amazon Redshift aprovisionados en su Cuenta de AWS.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
s3_ GetBucketEncryption	Recopila una instantánea que muestra la configuración de cifrado predeterminada para sus buckets de S3. Cuando utiliza esta API como origen de datos, no necesita proporcionar el nombre de un bucket de S3 específico. En su lugar, Audit Manager utiliza la operación `ListBuckets` para enumerar todos los bucket. Por cada bucket que aparece en la lista, Audit Manager realiza la operación `GetBucketEncryption` con el fin de generar una prueba para ese recurso. Audit Manager solo puede proporcionar el estado de cifrado de los buckets que se crearon al mismo tiempo Región de AWS que su evaluación. Si necesita ver el estado de cifrado de todos sus depósitos de S3 en varios Regiones de AWS, le recomendamos que cree una evaluación Región de AWS en cada uno de los depósitos de S3.
s3_ ListBuckets	Obtenga una lista de los depósitos S3 de su. Cuenta de AWS
sns_ ListTopics	Obtenga una lista de los temas de SNS en su. Cuenta de AWS
sqs_ ListQueues	Obtenga una lista de las colas de SQS de su. Cuenta de AWS

Llamadas a la API paginadas

Muchas Servicios de AWS recopilan y almacenan una gran cantidad de datos. Como resultado, cuando una llamada a la API `get`, `describe` o `list` intenta devolver sus datos, pueden producirse muchos resultados. Si la cantidad de datos es demasiado grande para devolverla en una sola respuesta, los resultados se pueden dividir en partes más fáciles de gestionar mediante el uso de la paginación. Esto divide los resultados en «páginas» de datos, lo que facilita el manejo de las respuestas.

Algunas de las llamadas a la API que admite Audit Manager están paginadas. Esto significa que al principio devuelven resultados parciales y requieren que las solicitudes posteriores devuelvan todo el conjunto de resultados. Por ejemplo, la operación DescribeDBInstances de Amazon RDS devuelven

hasta 100 instancias a la vez y se necesitan solicitudes posteriores para devolver la siguiente página de resultados.

Audit Manager admite las llamadas paginadas a la API como origen de datos para la recopilación de pruebas desde el 8 de marzo de 2023. Antes, si se utilizaba una llamada a la API paginada como origen de datos, en la respuesta a la API solo se devolvía un subconjunto de sus recursos (hasta 100 resultados). Ahora, Audit Manager llama a la operación de la API paginada varias veces y obtiene cada página de resultados hasta que se devuelven todos los recursos. A continuación, Audit Manager captura una instantánea de la configuración para cada recurso y la guarda como prueba. Como ahora todo tu conjunto de recursos se incluye en la respuesta de la API, es probable que notes un aumento en la cantidad de pruebas recopiladas.

Audit Manager gestiona automáticamente la paginación de las llamadas a la API. Si crea un control personalizado que utiliza una llamada a la API paginada como origen de datos, no necesita especificar ningún parámetro de paginación.

Las llamadas a la API se utilizan en el marco estándar de AWS License Manager

Audit Manager utiliza una actividad personalizada llamada `GetLicenseManagerSummary` para recopilar pruebas en el marco estándar AWS License Manager. Esta actividad llama a las siguientes tres API de License Manager:

- ListLicenseConfigurations
- ListAssociationsForLicenseConfiguration
- ListUsageForLicenseConfiguration

Los datos que se devuelven se convierten luego en pruebas y se adjuntan a los controles pertinentes de la evaluación.

Ejemplo

Supongamos que utiliza dos productos con licencia (SQL Service 2017 y Oracle Database Enterprise Edition). En primer lugar, la `GetLicenseManagerSummary` actividad llama a la ListLicenseConfigurationsAPI, que proporciona detalles de las configuraciones de licencia de su cuenta. A continuación, añade datos contextuales adicionales para cada configuración de licencia. Para ello, llama a ListUsageForLicenseConfigurationy ListAssociationsForLicenseConfiguration. Por último, convierte los datos de configuración de la licencia en pruebas y los adjunta a los controles respectivos del marco (4.5: licencia gestionada por el cliente para SQL Server 2017 y 3.0.4: licencia gestionada por el cliente para Oracle Database Enterprise Edition).

Si utiliza un producto con licencia que no está cubierto por ninguno de los controles del marco, los datos de configuración de la licencia se adjuntan como evidencia del siguiente control: 5.0: Licencia gestionada por el cliente para otras licencias.

AWS CloudTrail nombres de eventos compatibles con AWS Audit Manager

Puede capturar eventos AWS CloudTrail de administración y eventos de servicio global como evidencia en Audit Manager. Para ello, especifique el nombre del CloudTrail evento como palabra clave de mapeo de fuentes de datos al crear un control personalizado.

> **Note**
>
> Audit Manager captura eventos de administración y servicio global solamente. Los eventos de datos y los eventos de información no están disponibles como prueba. Para obtener más información sobre los distintos tipos de CloudTrail eventos, consulte CloudTrail los conceptos en la Guía delAWS CloudTrail usuario.

Como excepción a lo anterior, Audit Manager no admite los siguientes CloudTrail eventos:

- kms_ GenerateDataKey
- kms_Decrypt
- sts_ AssumeRole
- kinesisvideo_ GetDataEndpoint
- kinesisvideo_ GetSignalingChannelEndpoint
- kinesisvideo_ DescribeSignalingChannel
- kinesisvideo_ DescribeStream

A partir del 11 de mayo de 2023, Audit Manager ya no admite CloudTrail eventos de solo lectura como palabras clave para la recopilación de pruebas. Eliminamos un total de 3135 palabras clave de solo lectura. Como tanto los clientes como los Servicios de AWS realizan llamadas de lectura a las API, los eventos de solo lectura son ruidosos. Como resultado, las palabras clave de solo lectura recopilan una gran cantidad de pruebas que no son fiables ni relevantes para las auditorías. Las palabras clave de solo lectura incluyen `ListDescribe`, y las llamadas a la `Get` API (por ejemplo, GetObjecty ListBucketspara Amazon S3). Si utilizó una de estas palabras clave para la recopilación de pruebas, no tiene que realizar ninguna acción. Las palabras clave se eliminaron automáticamente

de la consola de Audit Manager y de sus evaluaciones, y ya no se recopilan pruebas de estas palabras clave.

Configuración de AWS Audit Manager

Puede revisar y configurar los ajustes de AWS Audit Manager en cualquier momento.

Para acceder a la configuración

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija Configuración.

Está disponible la siguiente configuración:

- Configuración general
  - Permisos
  - Cifrado de datos
  - Administrador delegado (opcional)
  - AWS Config (opcional)
  - Centro de seguridad (opcional)
  - Desactivar AWS Audit Manager
- Ajustes de evaluación
  - Propietarios de auditoría predeterminados (opcional)
  - Destino del informe de evaluación (opcional)
  - Notificaciones (opcional)
- Configuración del buscador de evidencias
  - Buscador de evidencias (opcional)
  - Destino de exportación (opcional)

Configuración general

La pestaña de configuración General es la vista predeterminada de la página de configuración de la consola de Audit Manager. Utilice esta pestaña para revisar y actualizar la configuración general de Audit Manager.

Temas

Permisos

AWS Audit Manager utiliza un rol vinculado a servicios para conectarse a orígenes de datos en su nombre. Para obtener más información, consulte Uso de funciones vinculadas a servicios para AWS Audit Manager.

Para revisar los datos relativos al rol vinculado al servicio que utiliza Audit Manager, seleccione Ver el permiso del rol vinculado al servicio de IAM.

Para obtener más información acerca los roles vinculados a servicios, consulte Uso de roles vinculados a servicios en la Guía del usuario de IAM.

Cifrado de datos

Audit Manager crea automáticamente una Clave administrada de AWS única para el almacenamiento seguro de sus datos. De forma predeterminada, los datos de Audit Manager se cifran con esta clave KMS. Como alternativa, si desea personalizar la configuración de cifrado de datos, puede especificar su propia clave de cifrado simétrico gestionada por el cliente. Usar su propia Clave de KMS le da más flexibilidad, incluida la capacidad de crear, rotar y desactivar claves.

> **Important**
>
> Para generar informes de evaluación y exportar correctamente los resultados de las búsquedas del buscador de evidencias, la clave gestionada por el cliente (si la proporciona) debe figurar en la misma Región de AWS que la de su evaluación. Para obtener una lista de regiones de Audit Manager, consulte AWS Audit Manager Puntos de conexión y cuotas de en la Referencia general de Amazon Web Services.

Puede actualizar la configuración de cifrado de datos mediante la consola de Audit Manager, AWS Command Line Interface (AWS CLI) o la API de Audit Manager.

Audit Manager console

Para actualizar la configuración de cifrado de datos (consola)

1. En la pestaña de ajustes General, vaya a la sección Cifrado de datos.
2. Para usar la clave KMS predeterminada que proporciona Audit Manager, desactive la casilla Personalizar la configuración de cifrado (avanzada).
3. Para utilizar una clave administrada por el cliente, active la casilla de verificación Personalizar la configuración de cifrado (avanzada). Puede elegir entonces una clave KMS existente o crear una nueva.

AWS CLI

Para actualizar la configuración de cifrado de datos (AWS CLI)

Ejecute el comando update-settings y utilice el parámetro `--kms-key` para especificar su propia clave gestionada por el cliente.

En el siguiente ejemplo, reemplace el *`texto del marcador de posición`* con su propia información.

```
aws auditmanager update-settings --kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Audit Manager API

Para actualizar la configuración de cifrado de datos (API)

Llame a la operación UpdateSettings y utilice el parámetro kmsKey para especificar su propia clave administrada por el cliente.

Para obtener más información, seleccione uno de los enlaces anteriores para obtener más información en la Referencia de la API de Audit Manager. Esto incluye información sobre cómo utilizar esta operación y los parámetros en uno de los SDK de AWS específicos del lenguaje.

> **Note**
>
> Al cambiar la configuración de cifrado de datos de Audit Manager, estos cambios se aplican a cualquier evaluación nueva que cree. Esto incluye todos los informes de evaluación y las exportaciones del buscador de evidencias que cree a partir de sus nuevas evaluaciones. Los cambios no se aplican a las evaluaciones existentes que creó antes de cambiar la configuración del cifrado. Esto incluye los nuevos informes de evaluación y las exportaciones a CSV que cree a partir de las evaluaciones existentes, además de los informes de evaluación y las exportaciones a CSV existentes. Las evaluaciones existentes (y todos sus informes de evaluación y exportaciones a CSV) siguen utilizando la antigua clave KMS. Si la identidad de IAM que genera el informe de evaluación no puede usar la antigua clave de KMS, concede permisos a nivel de política de claves. Para obtener instrucciones, consulte Permitir que los usuarios de otras cuentas utilicen una clave KMS en la Guía para desarrolladores de AWS Key Management Service.

Para obtener instrucciones sobre cómo crear claves, consulte Creación de claves en la Guía del usuario de AWS Key Management Service.

Administrador delegado (opcional)

Si utiliza AWS Organizations y desea habilitar la compatibilidad con varias cuentas para Audit Manager, puede designar una cuenta de miembro de su organización como administrador delegado de Audit Manager.

Requisitos previos

- Su cuenta debe formar parte de una organización. Para obtener más información, consulte Crear y administrar una organización en la Guía del usuario de AWS Organizations.
- Antes de designar un administrador delegado, debe habilitar todas las características de su organización. También debe configurar los ajustes del centro de seguridad de su organización. De esta forma, Audit Manager puede recopilar evidencias del centro de seguridad de las cuentas de sus miembros.
- La cuenta de administrador delegado debe tener acceso a la clave KMS que proporcionó al configurar Audit Manager. Para revisar y cambiar la configuración del cifrado, consulte Cifrado de datos.

Cuestiones importantes para los administradores delegados en Audit Manager

Tome nota de los siguientes factores que definen cómo funciona el administrador delegado en Audit Manager:

Uso de la cuenta de administración

No puede usar su cuenta de administración AWS Organizations como administrador delegado en Audit Manager.

Utilizar administradores delegados en varias Regiones de AWS

Si desea habilitar Audit Manager en más de una Región de AWS, debe designar una cuenta de administrador delegado por separado en cada región. En la configuración de Audit Manager, debe usar la misma cuenta de administrador delegado en todas las regiones.

Tarea de limpieza del buscador de evidencias

Antes de usar su cuenta de administración para eliminar o cambiar un administrador delegado, asegúrese de que la cuenta de administrador delegado actual inicie sesión en Audit Manager y deshabilite el buscador de evidencias. Al deshabilitar el buscador de evidencias, se elimina automáticamente el almacén de datos de eventos que se creó en la cuenta al habilitar el buscador de evidencias.

Si esta tarea no se completa, el almacén de datos del evento permanece en su cuenta. En este caso, recomendamos que el administrador delegado original utilice CloudTrail Lake para eliminar el almacén de datos de eventos manualmente.

Esta tarea de limpieza es necesaria para garantizar que no acabe con varios almacenes de datos de eventos. Audit Manager ignora un almacén de datos de eventos no utilizado después de eliminar o cambiar una cuenta de administrador delegado. Sin embargo, si no elimina el almacén de datos de eventos no utilizado, CloudTrail Lake seguirá incurriendo en costes de almacenamiento para el almacén de datos de eventos.

Eliminación de datos

Al eliminar una cuenta de administrador delegado de Audit Manager, los datos de esa cuenta no se eliminan. Si desea eliminar los datos de los recursos de una cuenta de administrador delegado, debe realizar esa tarea por separado antes de eliminar la cuenta. También puede hacer lo siguiente en la consola de Audit Manager. O puede utilizar una de las operaciones de eliminación de API proporcionadas por Audit Manager. Para obtener una lista de las operaciones de eliminación disponibles, consulte Eliminación de datos de Audit Manager.

En este momento, Audit Manager no ofrece la opción de eliminar las evidencias de un administrador delegado específico. En su lugar, cuando su cuenta de administración anula el registro de Audit Manager, realizamos una limpieza de la cuenta de administrador delegado actual en el momento de anular el registro.

Para obtener soluciones a los problemas comunes de las organizaciones y los administradores delegados en Audit Manager, consulte Solución de problemas AWS Organizations y del administrador delegado.

Administrar una cuenta de administrador delegado para Audit Manager

Puede revisar y cambiar la configuración de su cuenta de administrador delegado de la siguiente manera.

Agregar un administrador delegado

Puede añadir un administrador delegado mediante la consola de Audit Manager, la AWS Command Line Interface (AWS CLI) o la API de Audit Manager.

> **Note**
>
> Tras añadir un administrador delegado en la configuración de Audit Manager, su cuenta de administración ya no podrá crear evaluaciones adicionales en Audit Manager. Además, la recopilación de evidencias se detiene para cualquier evaluación existente creada por la cuenta de administración. Audit Manager recopila y adjunta evidencias a la cuenta de administrador delegado, que es la cuenta principal para gestionar las evaluaciones de la organización.

Audit Manager console

Para agregar un administrador delegado (consola)

1. En la pestaña de configuración General, vaya a la sección Administrador delegado.
2. En ID de cuenta de administrador delegado, introduzca el ID de cuenta del administrador delegado.
3. Elija Delegar.

AWS CLI

Para agregar un administrador delegado (AWS CLI)

Ejecute el comando register-organization-admin-account y utilice el parámetro `--admin-account-id` para especificar el ID de cuenta del administrador delegado.

En el siguiente ejemplo, reemplace el *texto del marcador de posición* con su propia información.

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

Para agregar un administrador delegado actual (API)

Llame a la operación RegisterOrganizationAdminAccount y utilice el parámetro adminAccountId para especificar el ID de cuenta del administrador delegado.

Para obtener más información, seleccione uno de los enlaces anteriores para obtener más información en la Referencia de la API de Audit Manager. Esto incluye información sobre cómo utilizar esta operación y los parámetros en uno de los SDK de AWS específicos del lenguaje.

Cambiar un administrador delegado

Puede cambiar un administrador delegado mediante la consola de Audit Manager, la AWS Command Line Interface (AWS CLI) o la API de Audit Manager.

> **Warning**
>
> Cuando cambia de administrador delegado, sigue teniendo acceso a las evidencias que recopiló anteriormente con la antigua cuenta de administrador delegado. Sin embargo, Audit Manager deja de recopilar y adjuntar evidencias a la antigua cuenta de administrador delegado.

Audit Manager console

Para cambiar el administrador delegado actual (consola)

1. (Opcional) Si el administrador delegado actual (cuenta A) ha habilitado el buscador de evidencias, lleve a cabo la siguiente tarea de limpieza:

   - Antes de asignar la cuenta B como nueva administradora delegada, asegúrese de que la cuenta A inicie sesión en Audit Manager y deshabilite el buscador de evidencias.

     Al deshabilitar el buscador de evidencias, se elimina automáticamente el almacén de datos de eventos que se creó cuando la cuenta A habilitó el buscador de evidencias. Si no completa este paso, la cuenta A debe ir a CloudTrail Lake y debe eliminar el almacén de datos de eventos manualmente. De lo contrario, el almacén de datos del evento permanecerá en la cuenta A y seguirá incurriendo en gastos de almacenamiento de CloudTrail Lake.
2. En la pestaña de configuración General, vaya a la sección Administrador delegado y elija Eliminar.
3. En la ventana emergente que aparece, seleccione Eliminar para confirmar.
4. En ID de cuenta de administrador delegado, introduzca el ID de cuenta del nuevo administrador delegado.
5. Elija Delegar.

AWS CLI

Antes de comenzar

Si el administrador delegado actual (cuenta A) ha activado el buscador de evidencias, lleve a cabo la siguiente tarea de limpieza:

Antes de asignar la cuenta B como nueva administradora delegada, asegúrese de que la cuenta A inicie sesión en Audit Manager y deshabilite el buscador de evidencias.

Al deshabilitar el buscador de evidencias, se elimina automáticamente el almacén de datos de eventos que se creó cuando la cuenta A habilitó el buscador de evidencias. Si no completa este paso, la cuenta A debe ir a CloudTrail Lake y debe eliminar el almacén de datos de eventos manualmente. De lo contrario, el almacén de datos del evento permanecerá en la cuenta A y seguirá incurriendo en gastos de almacenamiento de CloudTrail Lake.

Para cambiar el administrador delegado actual (AWS CLI)

Primero, ejecute el comando deregister-organization-admin-account y utilice el parámetro `--admin-account-id` para especificar el ID de cuenta del administrador delegado actual.

En el siguiente ejemplo, reemplace el *`texto del marcador de posición`* con su propia información.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

A continuación, ejecute el comando register-organization-admin-account y utilice el parámetro `--admin-account-id` para especificar el ID de cuenta del nuevo administrador delegado.

En el siguiente ejemplo, reemplace el *`texto del marcador de posición`* con su propia información.

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

Antes de comenzar

Si el administrador delegado actual (cuenta A) ha activado el buscador de evidencias, lleve a cabo la siguiente tarea de limpieza:

Antes de asignar la cuenta B como nueva administradora delegada, asegúrese de que la cuenta A inicie sesión en Audit Manager y deshabilite el buscador de evidencias.

Al deshabilitar el buscador de evidencias, se elimina automáticamente el almacén de datos de eventos que se creó cuando la cuenta A habilitó el buscador de evidencias. Si no completa este paso, la cuenta A debe ir a CloudTrail Lake y debe eliminar el almacén de datos de eventos manualmente. De lo contrario, el almacén de datos del evento permanecerá en la cuenta A y seguirá incurriendo en gastos de almacenamiento de CloudTrail Lake.

Para cambiar el administrador delegado (API) actual

En primer lugar, llame a la operación DeregisterOrganizationAdminAccount y utilice el parámetro AdminAccountID para especificar el ID de cuenta del administrador delegado actual.

A continuación, llame a la operación RegisterOrganizationAdminAccount y utilice el parámetro adminAccountId para especificar el ID de cuenta del nuevo administrador delegado.

Para obtener más información, seleccione uno de los enlaces anteriores para obtener más información en la Referencia de la API de Audit Manager. Esto incluye información sobre cómo utilizar esta operación y los parámetros en uno de los SDK de AWS específicos del lenguaje.

Eliminar un administrador delegado

Puede añadir un administrador delegado mediante la consola Audit Manager, la AWS Command Line Interface (AWS CLI) o la API Audit Manager.

> **Warning**
>
> Cuando elimina a un administrador delegado, continúa teniendo acceso a la evidencia que recopiló previamente en esa cuenta de administrador delegado. Sin embargo, Audit Manager deja de recopilar y adjuntar evidencias a la antigua cuenta de administrador delegado.

Audit Manager console

Para eliminar el administrador delegado actual (consola)

1. (Opcional) Si el administrador delegado actual ha activado el buscador de evidencias, lleve a cabo la siguiente tarea de limpieza:

   - Asegúrese de que la cuenta de administrador delegado actual inicie sesión en Audit Manager y desactive el buscador de evidencias.

     Al deshabilitar el buscador de evidencias, se elimina automáticamente el almacén de datos de eventos que se creó en la cuenta cuando habilitaron el buscador de evidencias. Si no se completa este paso, la cuenta de administrador delegado debe usar CloudTrail Lake para eliminar el almacén de datos de eventos manualmente. De lo contrario, el almacén de datos del evento permanecerá en su cuenta y seguirá incurriendo en gastos de almacenamiento de CloudTrail Lake.
2. En la pestaña de configuración General, vaya a la sección Administrador delegado y elija Eliminar.
3. En la ventana emergente que aparece, seleccione Eliminar para confirmar.

AWS CLI

Antes de comenzar

Si el administrador delegado actual ha activado el buscador de evidencias, lleve a cabo la siguiente tarea de limpieza:

Asegúrese de que la cuenta de administrador delegado actual inicie sesión en Audit Manager y desactive el buscador de evidencias.

Al deshabilitar el buscador de evidencias, se elimina automáticamente el almacén de datos de eventos que se creó en la cuenta cuando habilitaron el buscador de evidencias. Si no se completa este paso, la cuenta de administrador delegado debe usar CloudTrail Lake para eliminar el almacén de datos de eventos manualmente. De lo contrario, el almacén de datos del evento permanecerá en su cuenta y seguirá incurriendo en gastos de almacenamiento de CloudTrail Lake.

Para eliminar al administrador delegado actual (AWS CLI)

ejecute el comando deregister-organization-admin-account y utilice el parámetro `--admin-account-id` para especificar el ID de cuenta del administrador delegado.

En el siguiente ejemplo, reemplace el *`texto del marcador de posición`* con su propia información.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Audit Manager API

Antes de comenzar

Si el administrador delegado actual ha activado el buscador de evidencias, lleve a cabo la siguiente tarea de limpieza:

Asegúrese de que la cuenta de administrador delegado actual inicie sesión en Audit Manager y desactive el buscador de evidencias.

Al deshabilitar el buscador de evidencias, se elimina automáticamente el almacén de datos de eventos que se creó en la cuenta cuando habilitaron el buscador de evidencias. Si no se completa este paso, la cuenta de administrador delegado debe usar CloudTrail Lake para eliminar el almacén de datos de eventos manualmente. De lo contrario, el almacén de datos del evento

permanecerá en su cuenta y seguirá incurriendo en gastos de almacenamiento de CloudTrail Lake.

Para eliminar el administrador delegado actual (API)

Llame a la operación DeregisterOrganizationAdminAccount y utilice el parámetro adminAccountID para especificar el ID de cuenta del administrador delegado.

Para obtener más información, seleccione uno de los enlaces anteriores para obtener más información en la Referencia de la API de Audit Manager. Esto incluye información sobre cómo utilizar esta operación y los parámetros en uno de los SDK de AWS específicos del lenguaje.

AWS Config (opcional)

Puede permitir que Audit Manager recopile las conclusiones de AWS Config. Cuando AWS Config está habilitado, Audit Manager puede capturar instantáneas del estado de seguridad de sus recursos informando de los resultados de las comprobaciones de reglas directamente desde AWS Config. Le recomendamos que habilite AWS Config para lograr una experiencia óptima en Audit Manager.

Para habilitar AWS Config, seleccione AWS ConfigHabilitar para ir a ese servicio. Para obtener instrucciones sobre cómo habilitar AWS Config, consulte Configuración de AWS Config en la Guía para desarrolladores de AWS Config.

Centro de seguridad (opcional)

Puede permitir que Audit Manager importe las conclusiones de AWS Security Hub de las normas de conformidad compatibles. Cuando Security Hub está habilitado, Audit Manager puede capturar instantáneas del estado de seguridad de sus recursos mediante los resultados de las comprobaciones de seguridad directamente desde Security Hub. Le recomendamos que habilite Security Hub para lograr una experiencia óptima en Audit Manager.

Para habilitar Security Hub, seleccione Habilitar Security Hub para ir a ese servicio. Para obtener instrucciones acerca de cómo habilitar Security Hub, consulte la Configuración de AWS Security Hub en la Guía del usuario de Security Hub.

Desactivar AWS Audit Manager

Puede deshabilitar Audit Manager si ya no desea utilizar el servicio. Al deshabilitar Audit Manager, también tiene la opción de eliminar todos los datos.

De forma predeterminada, los datos no se eliminan al deshabilitar Audit Manager. Los datos de sus evidencias se conservan durante dos años desde el momento de su creación. Sus demás recursos de Audit Manager (incluidas las evaluaciones, los controles personalizados y los marcos personalizados) se retienen indefinidamente y estarán disponibles si vuelve a habilitar Audit Manager en el futuro. Para obtener más información sobre la retención de datos, consulte Protección de datos en esta guía.

Si decide eliminar sus datos, Audit Manager eliminará todos los datos de evidencia junto con todos los recursos de Audit Manager que haya creado (incluidas las evaluaciones, los controles personalizados y los marcos personalizados). Todos sus datos se eliminarán en un plazo de siete días a partir de la deshabilitación de Audit Manager.

> ⚠ Warning
>
> - Al deshabilitar Audit Manager, se revoca su acceso y el servicio ya no recopila evidencias de ninguna evaluación existente. No puede acceder a ningún elemento del servicio a menos que vuelva a habilitar Audit Manager.
> - Eliminar todos los datos es una acción permanente. Si decide volver a habilitar Audit Manager en el futuro, sus datos no se podrán recuperar.

Puede deshabilitar Audit Manager mediante la consola de Audit Manager, la AWS Command Line Interface (AWS CLI) o la API de Audit Manager.

Audit Manager console

Para deshabilitar Audit Manager (consola)

1. En la pestaña Configuración general, vaya a la sección Deshabilitar AWS Audit Manager.
2. Elija Deshabilitar.
3. En la ventana emergente, revise su configuración actual de retención de datos.
    a. Para continuar con la selección actual, seleccione Deshabilitar Audit Manager.
    b. Para cambiar la selección actual, ejecute los pasos siguientes:
        i. Pulse Cancelar para volver a la página de configuración.
        ii. Para usar la configuración de retención de datos predeterminada, desactive Eliminar todos los datos. Esta selección retiene los datos relativos a las evidencias durante

dos años a partir del momento de su creación y conserva otros recursos de Audit Manager de forma indefinida.

iii. Para eliminar sus datos, active Eliminar todos los datos.

iv. Seleccione Deshabilitar y, a continuación, elija Deshabilitar Audit Manager para confirmar su elección.

AWS CLI

Antes de comenzar

Antes de deshabilitar Audit Manager, puede ejecutar el comando update-settings para establecer la política de retención de datos que prefiera. De forma predeterminada, Audit Manager retiene sus datos. Si desea solicitar la eliminación de sus datos, utilice el parámetro `--deregistration-policy` con el valor `deleteResources` establecido en`ALL`.

```
aws auditmanager update-settings --deregistration-policy deleteResources=ALL
```

Para deshabilitar Audit Manager (AWS CLI)

Cuando esté listo para deshabilitar Audit Manager, ejecute el comando deregister-account.

```
aws auditmanager deregister-account
```

Audit Manager API

Antes de comenzar

Antes de deshabilitar Audit Manager, puede utilizar la operación API UpdateSettings para configurar su política de retención de datos preferida. De forma predeterminada, Audit Manager retiene sus datos. Si desea eliminar sus datos, puede utilizar el atributo DeregistrationPolicy para solicitar la eliminación de los datos.

Para deshabilitar Audit Manager (API)

Cuando esté listo para deshabilitar Audit Manager, llame a la operación DeregisterAccount.

Para obtener más información, seleccione uno de los enlaces anteriores para obtener más información en la Referencia de la API de Audit Manager. Esto incluye información sobre el uso de estas operaciones y parámetros en un lenguaje específico de un SDK de AWS.

Para volver a habilitar Audit Manager después de deshabilitarlo

Vaya a la página de inicio del servicio Audit Manager y siga los pasos para configurar Audit Manager como un nuevo usuario. Para obtener más información, consulte Configuración de AWS Audit Manager.

Tip

- Si eligió eliminar sus datos al deshabilitar Audit Manager, debe esperar a que se eliminen los datos para poder volver a habilitar el servicio. En función de la cantidad de datos de la que disponga, esto puede tardar hasta siete días. Sin embargo, no dude en intentar volver a activar Audit Manager antes de esa fecha. En muchos casos, los datos se eliminan en tan solo una hora.
- Si optó por no eliminar sus datos al deshabilitar Audit Manager, sus evaluaciones actuales pasarán a un estado latente y, en consecuencia, dejarán de recopilar evidencias. Para volver a recopilar evidencias para una evaluación preexistente, edite la evaluación y seleccione Guardar sin realizar ningún cambio.

Ajustes de evaluación

Utilice esta pestaña para revisar y actualizar la configuración de su evaluación.

Temas

- Propietarios de auditoría predeterminados (opcional)
- Destino del informe de evaluación (opcional)
- Notificaciones (opcional)

Propietarios de auditoría predeterminados (opcional)

Puede especificar los propietarios de auditoría predeterminados que tienen acceso principal a sus evaluaciones en Audit Manager.

Puede actualizar esta configuración utilizando la consola de Audit Manager, AWS Command Line Interface (AWS CLI) o la API de Audit Manager.

Audit Manager console

Puede elegir una de las Cuentas de AWS que aparecen en la tabla o utilizar la barra de búsqueda para buscar otras Cuentas de AWS.

Para actualizar la configuración predeterminada de los propietarios de la auditoría (consola)

1. En la pestaña de configuración de la Evaluación, vaya a la sección Propietarios de auditoría predeterminados y seleccione Editar.
2. Para añadir un propietario de auditoría predeterminado, marque la casilla de verificación situada junto al nombre de cuenta en Propietario de auditoría.
3. Para eliminar un propietario de auditoría predeterminado, desmarque la casilla de verificación junto al nombre de la cuenta en Propietario de auditoría.
4. Cuando haya terminado, elija Guardar.

AWS CLI

Para actualizar la configuración predeterminada del propietario de la auditoría (AWS CLI)

Ejecute el comando update-settings y use el parámetro `--default-process-owners` para especificar un propietario de auditoría.

En el siguiente ejemplo, reemplace el *`texto del marcador de posición`* con su propia información. Tenga en cuenta que solo `roleType` puede ser. `PROCESS_OWNER`

```
aws auditmanager update-settings --default-process-owners
 roleType=PROCESS_OWNER,roleArn=arn:aws:iam::111122223333:role/Administrator
```

Audit Manager API

Para actualizar la configuración predeterminada del propietario de la auditoría (API)

Llame a la operación UpdateSettings y utilice el parámetro DefaultProcessOwners para especificar los propietarios de la auditoría predeterminados. Tenga en cuenta que solo `roleType` puede ser. `PROCESS_OWNER`

Para obtener más información sobre los propietarios de las auditorías, consulte Propietarios de las auditorías en la sección Conceptos y terminología de esta guía.

Destino del informe de evaluación (opcional)

Al generar un informe de evaluación, Audit Manager publica el informe en el bucket de S3 que elija. Este bucket de S3 se denomina destino del informe de evaluación. Puede elegir el bucket de Amazon S3 en el que Audit Manager almacena sus informes de evaluación.

Puede actualizar esta configuración utilizando la consola de Audit Manager, AWS Command Line Interface (AWS CLI) o la API de Audit Manager.

Audit Manager console

Para actualizar la configuración de destino de su informe de evaluación (consola)

1. En la pestaña de configuración de la Evaluación, vaya a la sección Destino del informe de evaluación.
2. Para utilizar un bucket de Amazon S3 existente, seleccione un nombre de bucket en el menú desplegable.
3. Para crear un nuevo bucket de Amazon S3, elija Crear nuevo bucket.
4. Cuando haya terminado, elija Guardar.

AWS CLI

Para actualizar la configuración de destino de su informe de evaluación (AWS CLI)

Ejecute el comando update-settings y utilice el parámetro `--default-assessment-reports-destination` para especificar un bucket de S3.

En el siguiente ejemplo, reemplace el *`texto del marcador de posición`* con su propia información:

```
aws auditmanager update-settings --default-assessment-reports-destination
 destinationType=S3,destination=s3://doc-example-destination-bucket
```

Audit Manager API

Para actualizar la configuración de destino de su informe de evaluación (API)

Llame a la operación UpdateSettings y use el parámetro defaultAssessmentReportsDestination para especificar un bucket de S3.

Para obtener más información sobre cómo crear un bucket de S3, consulte Crear un bucket en la Guía del usuario de Amazon S3.

Consejos de configuración para el destino de su informe de evaluación

Para garantizar la correcta generación del informe de evaluación, le recomendamos que compruebe las siguientes configuraciones para el destino del informe de evaluación.

Buckets de la misma región

Le recomendamos que utilice un bucket de S3 que se encuentre en la misma Región de AWS de su evaluación. Si utiliza un bucket y una evaluación de la misma región, el informe de evaluación puede incluir hasta 22 000 elementos de evidencias. Por el contrario, si utiliza un bucket y una evaluación entre regiones, solo se pueden incluir 3500 elementos de evidencias.

Región de AWS

La Región de AWS de la clave administrada por su cliente (si la ha proporcionado) debe coincidir con la región de su evaluación y el bucket de S3 de destino del informe de evaluación. Para obtener instrucciones sobre cómo cambiar la clave KMS, consulte Configuración de AWS Audit Manager, cifrado de datos. Para obtener instrucciones sobre cómo cambiar el bucket de S3, consulte Configuración de AWS Audit Manager, destino del informe de evaluación. Para obtener una lista de regiones admitidas de Audit Manager, consulte AWS Audit Manager Puntos de conexión y cuotas de en la Referencia general de Amazon Web Services.

Cifrado de buckets de S3

Si el destino de su informe de evaluación tiene una política de buckets que requiere el cifrado del servidor (SSE) mediante SSE-KMS, entonces, la clave de KMS utilizada en esa política de buckets debe coincidir con la clave de KMS que configuró en los ajustes de cifrado de datos de Audit Manager. Si no ha configurado una clave KMS en la configuración de Audit Manager y la política de buckets de destino de su informe de evaluación requiere SSE, asegúrese de que la política de buckets permita SSE-S3. Para obtener instrucciones sobre cómo configurar la clave KMS que se utiliza para el cifrado de datos, consulte Configuración del cifrado de datos.

Buckets de S3 entre cuentas

La consola de Audit Manager no admite el uso de un bucket de S3 entre cuentas como destino del informe de evaluación. Es posible especificar un bucket entre cuentas como destino del informe de evaluación mediante la AWS CLI o una de las AWS SDK, pero por motivos de simplicidad, le recomendamos que no lo haga. Si opta por utilizar un bucket de S3 entre cuentas como destino del informe de evaluación, tenga en cuenta las siguientes cuestiones.

- De forma predeterminada, los objetos de S3 (como los informes de evaluación) son propiedad de la Cuenta de AWS que carga el objeto. Puede utilizar la configuración de Propiedad de objetos de S3 para cambiar este comportamiento predeterminado, de modo que cualquier nuevo objeto escrito por cuentas con la lista de control de acceso (ACL) predefinida `bucket-owner-full-control` se convierta automáticamente en propiedad del propietario del bucket.

  Aunque no es obligatorio, le recomendamos que realice los siguientes cambios en la configuración del bucket entre cuentas. Al realizar estos cambios, se garantiza que el propietario del bucket tenga el control total de los informes de evaluación que usted publique en su bucket.

  - Establezca la propiedad del objeto del bucket de S3 en el propietario del bucket preferido, en lugar de en el escritor de objetos predeterminado
  - Añada una política de buckets para asegurarse de que los objetos cargados en ese bucket tengan la ACL `bucket-owner-full-control`

- Para permitir que Audit Manager publique informes en un bucket de S3 entre cuentas, debe añadir la siguiente política de buckets de S3 al destino de su informe de evaluación. Sustituya el *`texto del marcador`* de posición por su propia información. El elemento `Principal` de esta política es el usuario o el rol propietario de la evaluación y crea el informe de la evaluación. El `Resource` especifica el bucket de S3 entre cuentas en el que se publica el informe.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account assessment report publishing",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
          },
          "Action": [
              "s3:ListBucket",
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetBucketLocation",
              "s3:PutObjectAcl",
              "s3:DeleteObject"
          ],
          "Resource": [
```

```
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
            ]
        }
    ]
}
```

Notificaciones (opcional)

Audit Manager puede enviar notificaciones al tema de Amazon SNS que especifique en esta configuración. Si está suscrito a ese tema de SNS, recibirá notificaciones cuando inicie sesión en Audit Manager.

Puede actualizar esta configuración utilizando la consola de Audit Manager, AWS Command Line Interface (AWS CLI) o la API de Audit Manager.

Audit Manager console

Para actualizar la configuración de notificaciones (consola)

1. En la pestaña de configuración de la Evaluación, vaya a la sección Notificaciones.
2. Para utilizar un tema de SNS existente, seleccione el nombre del tema en el menú desplegable.
3. Para crear un nuevo tema de SNS, elija Crear nuevo tema.
4. Cuando haya terminado, elija Guardar.

AWS CLI

Para actualizar la configuración de las notificaciones (AWS CLI)

Ejecute el comando update-settings y utilice el parámetro `--sns-topic` para especificar un tema de SNS.

En el siguiente ejemplo, reemplace el *texto del marcador de posición* con su propia información:

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-assessment-topic
```

Audit Manager API

Para actualizar la configuración de las notificaciones (API)

Llame a la operación UpdateSettings y utilice el parámetro snsTopic para especificar un tema de SNS.

> **Note**
>
> Puede utilizar un tema de SNS estándar o un tema de SNS FIFO (primero en entrar, primero en salir). Aunque Audit Manager admite el envío de notificaciones a temas de FIFO, no se garantiza el orden en que se envían los mensajes.
> Si desea utilizar un tema de Amazon SNS que no sea de su propiedad, configure su política de (IAM) de AWS Identity and Access Management para esto. Más específicamente, debe configurarlo para permitir la publicación desde el nombre de recurso de Amazon (ARN) del tema. Para obtener más información sobre IAM, consulte Gestión de identidades y accesos para AWS Audit Manager.

Para obtener más información sobre la lista de acciones que invocan notificaciones en Audit Manager, consulte Notificaciones de AWS Audit Manager.

Para obtener instrucciones sobre cómo crear un tema de Amazon SNS, consulte Crear un tema de Amazon SNS en la Guía del usuario de Amazon SNS.

Configuración del buscador de evidencias

Utilice esta pestaña para revisar y actualizar la configuración del buscador de evidencias.

Temas

- Buscador de evidencias (opcional)
- Destino de exportación (opcional)

Buscador de evidencias (opcional)

Recomendamos encarecidamente que habilite el buscador de evidencias. Es necesario activar esta característica si desea realizar consultas de búsqueda sobre sus evidencias.

Siga estos pasos para habilitar, deshabilitar o comprobar el estado del buscador de evidencias.

Habilitar el buscador de evidencias

Debe habilitar el buscador de evidencias en cada Región de AWS donde desee buscar evidencias. Si es administrador delegado de Audit Manager, habilite el buscador de evidencias para buscar evidencias en todas las cuentas de los miembros de su organización.

Permisos necesarios para habilitar el buscador de evidencias

Para habilitar el buscador de evidencias, necesita permisos para crear y administrar un almacén de datos de eventos en CloudTrail Lake. Para utilizar la característica, necesita permisos para realizar consultas de CloudTrail Lake. Para ver un ejemplo de política de permisos que puede usar, consulte Permitir el acceso total del administrador.

Si necesita ayuda con los permisos, póngase en contacto con su administrador de AWS. Si es un administrador AWS, puede copiar la declaración de permiso requerida y adjuntarla a una política de IAM.

Solicitar habilitar el buscador de evidencias

Puede completar esta tarea utilizando la consola de Audit Manager, AWS Command Line Interface (AWS CLI) o la API de Audit Manager.

Audit Manager console

Para solicitar la habilitación del buscador de evidencias (consola)

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En la pestaña de configuración del buscador de evidencias, vaya a la sección Buscador de evidencias.
3. Seleccione Política de permisos obligatoria y, a continuación, Ver permisos de CloudTrail Lake para ver los permisos de búsqueda de evidencias necesarios. Si aún no tiene estos permisos, puede copiar esta declaración de política y adjuntarla a una política de IAM.
4. Elija Habilitar.
5. En la ventana emergente, seleccione Solicitud de habilitación.

AWS CLI

Para solicitar la activación del buscador de evidencias (AWS CLI)

Ejecute el comando update-settings con el parámetro `--evidence-finder-enabled`.

```
aws auditmanager update-settings --evidence-finder-enabled
```

Audit Manager API

Para solicitar la activación del buscador de evidencias (API)

Llame a la operación UpdateSettings y utilice el parámetro evidenceFinderEnabled.

Para obtener más información, seleccione uno de los enlaces anteriores para obtener más información en la Referencia de la API de Audit Manager. Esto incluye información sobre cómo utilizar esta operación y los parámetros en uno de los SDK de AWS específicos del lenguaje.

Confirme el estado del buscador de evidencias

Tras enviar la solicitud, se necesitarán hasta 10 minutos para habilitar el buscador de evidencias y crear un almacén de datos de eventos. En cuanto se crea el almacén de datos del evento, todas las evidencias nuevas se incorporan al almacén de datos del evento a partir de ahora.

Cuando el buscador de evidencias está habilitado y se crea el almacén de datos del evento, rellenamos el almacén de datos del evento recién creado con evidencias anteriores equivalentes a un máximo de dos años. Este proceso se realiza automáticamente y tarda hasta siete días en completarse.

Puede comprobar el estado actual del buscador de evidencias mediante la consola de Audit Manager, la AWS CLI o la API de Audit Manager.

Audit Manager console

Para ver el estado actual del buscador de evidencias (consola)

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija Configuración.
3. En Habilitar el buscador de evidencias (opcional), revise el estado actual.

Cada estado se define de la siguiente manera:

- El buscador de evidencias no está habilitado: aún no ha habilitado correctamente el buscador de evidencias.
- Ha solicitado habilitar el buscador de evidencias: su solicitud está pendiente de la creación del almacén de datos del evento.
- El buscador de evidencias está habilitado: se creó el almacén de datos del evento. A partir de ahora, puede utilizar el buscador de evidencias.

  Dependiendo de la cantidad de evidencias que tenga, tardará hasta siete días en rellenar el nuevo almacén de datos de eventos con los datos de las evidencias anteriores. Un panel de información azul indica que la reposición de datos está en curso. Mientras tanto, no dude en empezar a explorar el buscador de evidencias. Sin embargo, tenga en cuenta que no todos los datos están disponibles hasta que se complete la reposición.
- Ha solicitado desactivar el buscador de evidencias: su solicitud está pendiente de que se elimine el almacén de datos de eventos.
- Se ha deshabilitado el buscador de evidencias: el buscador de evidencias se ha deshabilitado permanentemente y se ha eliminado el almacén de datos del evento.

AWS CLI

Para ver el estado actual del buscador de evidencias (AWS CLI)

Ejecute el comando get-settings con el parámetro `--attribute` configurado como `EVIDENCE_FINDER_ENABLEMENT`.

```
aws auditmanager get-settings --attribute EVIDENCE_FINDER_ENABLEMENT
```

Esto devuelve la siguiente información:

enablementStatus

Este atributo muestra el estado actual del buscador de evidencias.

- `ENABLE_IN_PROGRESS`: ha solicitado habilitar el buscador de evidencias. Actualmente se está creando un almacén de datos de eventos para respaldar las consultas de los buscadores de evidencias.

- `ENABLED`: se creó un almacén de datos de eventos y se habilitó el buscador de evidencias. Le recomendamos que espere siete días hasta que el almacén de datos del evento se rellene con sus datos de evidencias anteriores. Mientras tanto, puede utilizar el buscador de evidencias, pero no todos los datos estarán disponibles hasta que se complete el proceso de relleno.
- `DISABLE_IN_PROGRESS`: ha solicitado desactivar el buscador de evidencias y su solicitud está pendiente de que se elimine el almacén de datos de eventos.
- `DISABLED`: ha deshabilitado permanentemente el buscador de evidencias y se ha eliminado el almacén de datos del evento. Después de este punto, no podrá volver a habilitar el buscador de evidencias.

backfillStatus

Este atributo muestra el estado actual de la reposición del buscador de evidencias.

- `NOT_STARTED`: la reposición aún no ha empezado.
- `IN_PROGRESS`: la reposición está en curso. Esto tarda hasta siete días en completarse, según la cantidad de evidencias.
- `COMPLETED`: la reposición ha finalizado. Todas sus evidencias anteriores ahora son consultables.

Audit Manager API

Para ver el estado actual del buscador de evidencias (API)

Llame a la operación GetSettings con el parámetro `attribute` establecido en `EVIDENCE_FINDER_ENABLEMENT`. Esto devuelve la siguiente información:

enablementStatus

Este atributo muestra el estado actual del buscador de evidencias.

- `ENABLE_IN_PROGRESS`: ha solicitado habilitar el buscador de evidencias. Actualmente se está creando un almacén de datos de eventos para respaldar las consultas de los buscadores de evidencias.
- `ENABLED`: se creó un almacén de datos de eventos y se habilitó el buscador de evidencias. Le recomendamos que espere siete días hasta que el almacén de datos del evento se rellene con sus datos de evidencias anteriores. Mientras tanto, puede utilizar el buscador de evidencias, pero no todos los datos estarán disponibles hasta que se complete el proceso de relleno.

- `DISABLE_IN_PROGRESS`: ha solicitado deshabilitar el buscador de evidencias y su solicitud está pendiente de que se elimine el almacén de datos de eventos.
- `DISABLED`: ha deshabilitado permanentemente el buscador de evidencias y se ha eliminado el almacén de datos del evento. Después de este punto, no podrá volver a habilitar el buscador de evidencias.

backfillStatus

Este atributo muestra el estado actual de la reposición del buscador de evidencias.

- `NOT_STARTED` significa que la reposición aún no ha empezado.
- `IN_PROGRESS` significa que la reposición está en curso. Esto tarda hasta siete días en completarse, según la cantidad de evidencias.
- `COMPLETED` significa que la reposición ha finalizado. Todas sus evidencias anteriores ahora son consultables.

Para obtener más información, consulte evidenceFinderEnablement en la Referencia de la API de Audit Manager.

Deshabilitar el buscador de evidencias

Si ya no desea utilizar el buscador de evidencias, puede deshabilitar esta característica en cualquier momento.

> **Warning**
>
> Al deshabilitar el buscador de evidencias, se elimina el almacén de datos de eventos de CloudTrail Lake que creó Audit Manager. Por consiguiente, no puede volver a habilitar la característica. Para volver a utilizar el buscador de evidencias después de deshabilitarlo, debe deshabilitar AWS Audit Manager y, a continuación, volver a habilitar el servicio por completo.

Permisos necesarios para deshabilitar el buscador de evidencias

Para deshabilitar el buscador de evidencias, necesita permisos para eliminar un almacén de datos de eventos en CloudTrail Lake. Para ver un ejemplo de política que puede utilizar, consulte Permisos para deshabilitar el buscador de evidencias.

Si necesita ayuda con los permisos, póngase en contacto con su administrador de AWS. Si es administrador de AWS, puede adjuntar la declaración de permiso requerida a una política de IAM.

Deshabilitar el buscador de evidencias

Puede completar esta tarea utilizando la consola de Audit Manager, AWS Command Line Interface (AWS CLI) o la API de Audit Manager.

Audit Manager console

Para deshabilitar el buscador de evidencias (consola)

1. En la sección Buscador de evidencias de la página de configuración de Audit Manager, seleccione Deshabilitar.
2. En la ventana emergente que aparece, introduzca **`Yes`** para confirmar su decisión.
3. Seleccione Solicitar deshabilitación.

AWS CLI

Para deshabilitar el buscador de evidencias (AWS CLI)

Ejecute el comando update-settings con el parámetro `--no-evidence-finder-enabled`.

```
aws auditmanager update-settings --no-evidence-finder-enabled
```

Audit Manager API

Para deshabilitar el buscador de evidencias (API)

Llame a la operación UpdateSettings y utilice el parámetro evidenceFinderEnabled.

Para obtener más información, seleccione uno de los enlaces anteriores para obtener más información en la Referencia de la API de Audit Manager. Esto incluye información sobre cómo utilizar esta operación y los parámetros en uno de los SDK de AWS específicos del lenguaje.

Destino de exportación (opcional)

Al ejecutar consultas en el buscador de evidencias, puede exportar los resultados de la búsqueda a un archivo CSV (valores separados por comas). Utilice esta configuración para elegir el bucket de S3 predeterminado en el que Audit Manager guarda los archivos exportados.

Puede actualizar esta configuración utilizando la consola de Audit Manager, AWS Command Line Interface (AWS CLI) o la API de Audit Manager.

> **Important**
>
> Su bucket de S3 debe tener la política de permisos requerida para permitir que CloudTrail escriba los archivos de exportación en él. Más específicamente, la política de buckets debe incluir una acción `s3:PutObject` y el ARN del bucket, además de incluir CloudTrail como entidad principal del servicio. Proporcionamos un ejemplo de política de permisos que puede utilizar. Para obtener instrucciones sobre cómo adjuntar esta política a su bucket de S3, consulte Añadir una política de buckets mediante la consola de Amazon S3.
> Para obtener más consejos, consulte los Consejos de configuración para su destino de exportación en esta página.

Audit Manager console

Para actualizar la configuración del destino de exportación (consola)

1. En la pestaña de configuración del buscador de evidencias, vaya a la sección Destino de exportación.
2. Elija una de las siguientes opciones:
   - Si quiere eliminar el bucket de S3 actual, seleccione Eliminar para borrar la configuración.
   - Si quiere guardar un bucket de S3 predeterminado por primera vez, continúe con el paso 3.
3. Especifique el bucket de S3 en el que desea almacenar los archivos exportados.
   - Seleccione Explorar S3 para elegir de una lista de sus buckets.
   - Como alternativa, puede introducir el URI del bucket en este formato: **`s3://bucketname/prefix`**

> **Tip**
>
> Para mantener el bucket de destino organizado, puede crear una carpeta opcional para sus exportaciones a CSV. Para ello, añada una barra (**/**) y un prefijo al valor del cuadro URI del recurso (por ejemplo, **`/evidenceFinderCSVExports`**). A continuación, Audit Manager incluirá este prefijo cuando añada el archivo CSV al bucket y Amazon S3 generará la ruta especificada por el prefijo. Para obtener más información acerca de los prefijos en Amazon S3, consulte Organizar objetos en la consola de Amazon S3 en la guía del usuario de Amazon Simple Storage Service.

4. Cuando haya terminado, elija Guardar.

Para obtener más información sobre cómo crear un bucket de S3, consulte Crear un bucket en la Guía del usuario de Amazon S3.

AWS CLI

Para actualizar la configuración del destino de exportación (AWS CLI)

Ejecute el comando update-settings y utilice el parámetro `--default-export-destination` para especificar un bucket de S3.

En el siguiente ejemplo, reemplace el *`texto del marcador de posición`* con su propia información:

```
aws auditmanager update-settings --default-export-destination
 destinationType=S3,destination=s3://doc-example-destination-bucket
```

Para obtener instrucciones sobre cómo crear un bucket de S3, consulte create-bucket en la Referencia de comandos de la AWS CLI.

Audit Manager API

Para actualizar la configuración del destino de exportación (API)

Llame a la operación UpdateSettings y use el parámetro defaultExportDestination para especificar un bucket de S3.

Para obtener instrucciones sobre cómo crear un bucket de S3, consulte CreateBucket en la Referencia de la API de Amazon S3.

Consejos de configuración para el destino de su exportación

Para garantizar una exportación de archivos correcta, le recomendamos que compruebe las siguientes configuraciones para el destino de su exportación.

Región de AWS

La Región de AWS de la clave administrada por su cliente (si la ha proporcionado) debe coincidir con la región de su evaluación. Para obtener instrucciones sobre cómo cambiar la clave KMS, consulte Configuración de cifrado de datos de Audit Manager.

Buckets de S3 entre cuentas

La consola de Audit Manager no admite el uso de un bucket de S3 entre cuentas como destino de su exportación. Es posible especificar un bucket entre cuentas mediante la AWS CLI o una de las AWS SDK, pero por motivos de simplicidad, le recomendamos que no lo haga. Si opta por utilizar un bucket de S3 entre cuentas como destino de su exportación, tenga en cuenta las siguientes cuestiones.

- De forma predeterminada, los objetos de S3 (como las exportaciones a CSV) son propiedad de la Cuenta de AWS que carga el objeto. Puede utilizar la configuración de Propiedad de objetos de S3 para cambiar este comportamiento predeterminado, de modo que cualquier nuevo objeto escrito por cuentas con la lista de control de acceso (ACL) predefinida `bucket-owner-full-control` se convierta automáticamente en propiedad del propietario del bucket.

  Aunque no es obligatorio, le recomendamos que realice los siguientes cambios en la configuración del bucket entre cuentas. Al realizar estos cambios, se garantiza que el propietario del bucket tenga el control total de los archivos exportados que publica en su bucket.

  - Establezca la propiedad del objeto del bucket de S3 en el propietario del bucket preferido, en lugar de en el escritor de objetos predeterminado
  - Añada una política de buckets para asegurarse de que los objetos cargados en ese bucket tengan la ACL `bucket-owner-full-control`
- Para permitir que Audit Manager exporte archivos a un depósito S3 entre cuentas, debe agregar la siguiente política de bucket de S3 a su bucket de destino de exportación. Sustituya el *`texto del marcador`* de posición por su propia información. El `Principal` elemento de esta política es el usuario o rol propietario de la evaluación y exporta el archivo. El `Resource` especifica el bucket de S3 entre cuentas al que se exporta el archivo.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account file exports",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
          },
          "Action": [
              "s3:ListBucket",
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetBucketLocation",
              "s3:PutObjectAcl",
              "s3:DeleteObject"
          ],
          "Resource": [
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
          ]
      }
  ]
}
```

Notificaciones de AWS Audit Manager

AWS Audit Manager puede notificarle las acciones de los usuarios a través de Amazon Simple Notification Service (Amazon SNS).

Audit Manager envía notificaciones cuando se produce uno de los siguientes eventos:

- El propietario de la auditoría delega un conjunto de controles para su revisión.
- Un delegado envía un conjunto de controles revisado al propietario de la auditoría.
- El propietario de la auditoría completa la revisión de un conjunto de controles.

Requisitos previos

Antes de configurar las notificaciones de Amazon SNS en Audit Manager, asegúrese de completar los pasos siguientes.

1. Cree un tema en Amazon SNS si aún no dispone de uno. Para obtener instrucciones, consulte el tema Creación de un Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.
2. Suscriba al menos un punto de enlace al tema. Por ejemplo, si desea recibir notificaciones por mensaje de texto, suscriba un punto de enlace de SMS al tema. Un punto de conexión de SMS es un número de teléfono móvil. Para recibir notificaciones por correo electrónico, suscriba un punto de enlace de correo electrónico al tema. Un punto de conexión de correo electrónico es una dirección de correo electrónico.

   Para obtener más información, consulte Introducción en la Guía para desarrolladores de Amazon Simple Notification Service.
3. (Opcional) Si su tema de AWS Key Management Service utiliza (AWS KMS) para el cifrado del servidor (SSE), tendrá que añadir permisos a la política de claves de AWS KMS key. Para ver un ejemplo de política que puede usar, consulte Permisos para una clave de KMS adjunta a un tema de SNS.

Configuración de notificaciones en AWS Audit Manager

Siga estos pasos para configurar notificaciones en AWS Audit Manager.

Para configurar notificaciones en la AWS Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. En el panel de navegación izquierdo, elija Configuración.
3. Especifique el tema de SNS que desea utilizar para recibir notificaciones desde Notificaciones: opcional.
   - Para utilizar un tema existente, seleccione el nombre del tema en el menú desplegable.
   - Para crear un tema nuevo, seleccione Crear tema nuevo. Esto lo llevará a la consola de Amazon SNS, donde podrá crear un tema.
4. Cuando haya terminado, elija Guardar.

> **Notas**
>
> - Puede utilizar un tema de SNS estándar o un tema de SNS FIFO (primero en entrar, primero en salir). Audit Manager admite el envío de notificaciones a temas de FIFO. Sin embargo, no se garantiza el orden en que se envían los mensajes.
> - Si desea utilizar un tema de Amazon SNS que no sea de su propiedad, debe configurar la política de (IAM) de AWS Identity and Access Management. Más específicamente, debe configurar su política para permitir la publicación desde el nombre de recurso de Amazon (ARN) del tema. Para obtener más información, consulte Administración de identidad y acceso para .

Solución de problemas

Para encontrar respuestas a preguntas y problemas comunes, consulte Solución de problemas relacionados con las notificaciones en la sección Solución de problemas de esta guía.

Solución de problemas en AWS Audit Manager

Puede utilizar la siguiente información para solucionar los problemas que pueden surgir al trabajar con AWS Audit Manager.

Si los problemas que se le presenten quedan fuera del ámbito de la siguiente información o continúan después de haber intentado resolverlos, póngase en contacto con AWS Support.

Temas

Solución de problemas de evaluación y recopilación de pruebas

Puede utilizar la información de esta página para resolver problemas comunes de evaluación y recopilación de pruebas en Audit Manager.

Temas

- Mis pruebas se generan a intervalos diferentes y no estoy seguro de la frecuencia con la que se recopilan
- ¿Qué ocurre si elimino una cuenta incluida en el ámbito de aplicación de mi organización?
- No puedo editar los servicios incluidos en el ámbito de mi evaluación
- ¿Cuál es la diferencia entre un servicio incluido y un tipo de origen de datos?
- Error al crear mi evaluación
- He desactivado Audit Manager y, a continuación, he vuelto a activarlo, y ahora mis evaluaciones preexistentes ya no recopilan pruebas

He creado una evaluación, pero aún no veo ninguna prueba

Si no ve ninguna prueba, es probable que no haya esperado al menos 24 horas después de crear la evaluación o que se trate de un error de configuración.

Le recomendamos que compruebe lo siguiente:

1. Asegúrese de que hayan pasado 24 horas desde que creó la evaluación. Las pruebas automatizadas pasan a estar disponibles las 24 horas después de crear la evaluación.
2. Asegúrese de utilizar Audit Manager de la misma forma Región de AWS en que Servicio de AWS que espera ver pruebas.
3. Si espera ver pruebas de conformidad procedentes de AWS Config y AWS Security Hub, asegúrese de que tanto la consola como la AWS Config de Security Hub muestren los resultados de estas comprobaciones. Los resultados de AWS Config y los de Security Hub deberían mostrarse en el mismo formato Región de AWS que utiliza Audit Manager.

Si sigue sin poder ver pruebas en su evaluación y no se debe a uno de estos problemas, compruebe las demás posibles causas que se describen en esta página.

Mi evaluación no consiste en recopilar pruebas de control de conformidad de AWS Security Hub

Si no ve las pruebas de verificación de conformidad de un AWS Security Hub control, podría deberse a uno de los siguientes problemas.

Falta la configuración en AWS Security Hub

Este problema puede deberse a que omitió algunos pasos de configuración cuando habilitó AWS Security Hub.

Asegúrese de haber activado Security Hub y de haber configurado los ajustes de la siguiente manera.

Confirmar la configuración de Security Hub para una sola Cuenta de AWS

Si utiliza una sola Cuenta de AWS, verifique lo siguiente:

- Confirme que ha activado AWS Config y configurado el registro de recursos para su cuenta .
- Confirme que ha activado el estándar de seguridad PCI DSS para su cuenta .
- Confirme que ha activado la configuración de resultados de control consolidados en Security Hub.

Confirmar la configuración de Security Hub para una organización

Si utiliza Organizations, compruebe lo siguiente:

- Confirme que ha activado AWS Config y configurado el registro de recursos para su organización.
- Confirme que ha activado el estándar de seguridad PCI DSS para todas las cuentas de los miembros de la organización.
- Confirme que ha activado la configuración de resultados de control consolidados en Security Hub.
- Confirme que la cuenta de administrador delegado que utiliza en Security Hub es la misma que utiliza en Audit Manager.
- Confirme que ha activado las cuentas de su organización como cuentas de miembro de Security Hub.

Se ha introducido incorrectamente un nombre de control de Security Hub en su **`ControlMappingSource`**

Cuando utiliza la API Audit Manager para crear un control personalizado, puede especificar un control de Security Hub como asignación de origen de datos para la recopilación de pruebas. Para ello, introduzca un ID de control como `keywordValue`.

Si no ve pruebas de verificación de conformidad de un control de Security Hub, es posible que el `keywordValue` se haya introducido incorrectamente en su `ControlMappingSource`. El

`keywordValue` distingue entre mayúsculas y minúsculas. Si la introduce de forma incorrecta, es posible que Audit Manager no reconozca esa regla. Como resultado, es posible que no recopile las pruebas de verificación de cumplimiento de ese control como se esperaba.

Para solucionar este problema, actualice el control personalizado y revise el `keywordValue`. El formato correcto de una palabra clave de Security Hub varía. Para mayor precisión, consulte la lista de palabras clave de control de Security Hub compatibles.

`AuditManagerSecurityHubFindingsReceiver`Falta la regla de Amazon EventBridge

Al activar Audit Manager, se crea y activa automáticamente una regla denominada `AuditManagerSecurityHubFindingsReceiver` en Amazon EventBridge. Esta regla permite a Audit Manager recopilar las conclusiones de Security Hub como pruebas.

Si esta regla no aparece ni habilitada en el Región de AWS lugar donde usa Security Hub, Audit Manager no podrá recopilar los resultados del Security Hub para esa región.

Para resolver este problema, vaya a la consola de EventBridge y confirme que la `AuditManagerSecurityHubFindingsReceiver` regla existe en su Cuenta de AWS Si la regla no existe, le recomendamos que desactive Audit Manager y, a continuación, vuelva a activar el servicio. Si esta acción no resuelve el problema o si la desactivación de Audit Manager no es una opción, pongáse en contacto con nosotros AWS Support para obtener ayuda.

AWS ConfigReglas vinculadas a servicios creadas por Security Hub

Tenga en cuenta que Audit Manager no recopila pruebas de las reglas vinculadasAWS Config a servicios que crea Security Hub. Se trata de un tipo específico de regla AWS Config gestionada que el servicio Security Hub habilita y controla. Security Hub crea estas reglas vinculadas a servicios en su ambiente AWS, incluso si ya existen otras instancias de las mismas reglas. Como resultado, para evitar la duplicación de pruebas, Audit Manager no admite la recopilación de pruebas a partir de las reglas vinculadas a los servicios.

Mi evaluación no consiste en recopilar pruebas de control de conformidad de AWS Config

Si no ve pruebas de comprobación del cumplimiento de una norma AWS Config ,podría deberse a uno de los siguientes problemas.

El identificador de la regla se ingresó incorrectamente en su **`ControlMappingSource`**

Cuando utiliza la API Audit Manager para crear un control personalizado, puede especificar una regla AWS Config como asignación de origen de datos para la recopilación de pruebas. Lo `keywordValue`que especifique depende del tipo de regla.

Si no ve pruebas de comprobación de cumplimiento para una regla AWS Config, podría ser que `keywordValue` se introdujo incorrectamente en su `ControlMappingSource`. El `keywordValue` distingue entre mayúsculas y minúsculas. Si la introduce de forma incorrecta, es posible que Audit Manager no reconozca la regla. Como consecuencia, es posible que no recopile evidencia de verificación de cumplimiento para esa regla según lo previsto.

Para solucionar este problema, actualice el control personalizado y revise el `keywordValue`.

- En el caso de las reglas personalizadas, asegúrese de que `keywordValue` tenga el prefijo `Custom_` seguido del nombre de la regla personalizada. El formato del nombre de la regla personalizada puede variar. Para mayor precisión, visite la AWS Configconsola para comprobar los nombres de las reglas personalizadas.
- En el caso de las reglas administradas, asegúrese de que `keywordValue` es el identificador de la regla en `ALL_CAPS_WITH_UNDERSCORES`. Por ejemplo, `CLOUDWATCH_LOG_GROUP_ENCRYPTED`. Para mayor precisión, consulte la lista de palabras clave de reglas administradas compatibles.

> **Note**
>
> En el caso de algunas reglas administradas, el identificador de la regla es diferente del nombre de la regla. Por ejemplo, el identificador de regla para restricted-ssh es `INCOMING_SSH_DISABLED`. Asegúrese de usar el identificador de la regla, no el nombre de la regla. Para buscar un identificador de regla, elija una regla de la lista de reglas administradas y busque su valor de identificador.

La regla es una regla vinculada a un servicio AWS Config

Puede usar reglas administradas y reglas personalizadas como asignación de origen de datos para la recopilación de pruebas. Sin embargo, Audit Manager no recopila pruebas de la mayoría de las reglas vinculadas a los servicios.

Solo hay dos tipos de reglas vinculadas a servicios de las que Audit Manager recopila pruebas:

- Reglas vinculadas a servicios de los paquetes de conformidad

- Reglas vinculadas a servicios de AWS Organizations

  Audit Manager no recopila pruebas de otras reglas vinculadas a servicios, específicamente de las reglas con un nombre de recurso de Amazon (ARN) que contenga el siguiente prefijo: `arn:aws:config:*:*:config-rule/aws-service-rule/...`

  La razón por la que Audit Manager no recopila pruebas de la mayoría de AWS Config las reglas vinculadas a los servicios es para evitar la duplicación de pruebas en sus evaluaciones. Una regla vinculada a un servicio es un tipo específico de regla administrada que permite a otros Servicios de AWS crear reglas AWS Config en su cuenta. Por ejemplo, algunos controles de Security Hub utilizan una regla AWS Config vinculada a un servicio para ejecutar controles de seguridad. Para cada control de Security Hub que utiliza una regla vinculada a un servicioAWS Config, Security Hub crea una instancia de la regla requerida AWS Config en su AWSentorno. Esto sucede incluso si la regla original ya existe en la cuenta. Por lo tanto, para evitar recopilar la misma evidencia de la misma regla dos veces, Audit Manager ignora la regla vinculada al servicio y no recopila evidencia a partir de ella.

AWS Config no está activado ni incluido como servicio dentro del ámbito

AWS Config debe estar habilitado en su región de Cuenta de AWS También debe incluirse como un servicio dentro del ámbito de su evaluación. Una vez que haya configurado AWS Config de esta manera, Audit Manager recopila pruebas cada vez que se realiza la evaluación de una AWS Config regla.

En primer lugar, asegúrese de haber activado AWS Config en su Cuenta de AWS. Para obtener instrucciones, consulte Habilitar y configurarAWS Config.

A continuación, asegúrese de incluir AWS Config como servicio en el ámbito de su evaluación. Para revisar los servicios actuales incluidos en el ámbito de su evaluación, consulte la pestaña Servicios de AWSRevisar una evaluación. Para editar la lista de servicios incluidos en una evaluación, consulte Editar Servicios de AWS servicios incluidos.

La regla AWS Config evaluó la configuración de un recurso antes de configurar la evaluación

Si la regla AWS Config está configurada para evaluar los cambios de configuración de un recurso específico, es posible que vea una discrepancia entre la evaluación AWS Config y la evidencia en Audit Manager. Esto ocurre si la evaluación de la regla se realizó antes de configurar el control en la evaluación de Audit Manager. En este caso, Audit Manager no genera pruebas hasta que el recurso subyacente vuelve a cambiar de estado y desencadena una reevaluación de la regla.

Como solución alternativa, puede navegar hasta la regla en la consola AWS Config y volver a evaluarla manualmente. Esto requiere una nueva evaluación de todos los recursos que pertenecen a esa regla.

Mi evaluación no consiste en recopilar pruebas de la actividad de los usuarios de AWS CloudTrail

Cuando utiliza la API Audit Manager para crear un control personalizado, puede especificar el nombre de un evento de CloudTrail como asignación de origen de datos para la recopilación de pruebas. Para ello, introduzca el nombre del evento como `keywordValue`.

Si no ve evidencia de la actividad del usuario en un evento de CloudTrail, es posible que `keywordValue` se haya introducido incorrectamente en su `ControlMappingSource`. El `keywordValue` distingue entre mayúsculas y minúsculas. Si la introduce de forma incorrecta, es posible que Audit Manager no reconozca el nombre del evento. Como resultado, es posible que no recopile las pruebas de la actividad del usuario en relación con ese evento según lo previsto.

Para solucionar este problema, actualice el control personalizado y revise el `keywordValue`. Asegúrese de que el evento esté escrito como `serviceprefix_ActionName`. Por ejemplo, `cloudtrail_StartLogging`. Para mayor precisión, revise el prefijo Servicio de AWS y los nombres de las acciones en la Referencia de autorización de servicio.

Mi evaluación no consiste en recopilar pruebas de datos de configuración para una llamada a la API de AWS

Cuando utiliza la API del Administrador de auditorías para crear un control personalizado, puede especificar una llamada a la API de AWS como asignación de origen de datos para la recopilación de pruebas. Para ello, debe introducir la llamada a la API como `keywordValue`.

Si no ve evidencia de los datos de configuración de una llamada a la API de AWS, es posible que haya introducido `keywordValue` incorrectamente en su `ControlMappingSource`. El `keywordValue` distingue entre mayúsculas y minúsculas. Si lo introduce de forma incorrecta, es posible que Audit Manager no reconozca la llamada a la API. Como resultado, es posible que no recopile pruebas de datos de configuración para esa llamada a la API según lo previsto.

Para solucionar este problema, actualice el control personalizado y revise el `keywordValue`. Asegúrese de que la llamada a la API esté escrita como `serviceprefix_ActionName`.

Por ejemplo, `iam_ListGroups`. Para mayor precisión, consulte la lista de llamadas a la API compatibles.

Mi evaluación no consiste en recopilar pruebas de otra Servicio de AWS

Si Servicio de AWS no se selecciona como parte del alcance de su evaluación, Audit Manager no recopila pruebas de los recursos relacionados con ese servicio. Este también es el caso si Servicio de AWS se selecciona pero no la ha activado en su entorno.

Si creó la evaluación a partir de un marco personalizado, puede editar los servicios incluidos en el ámbito de la evaluación. A continuación, puede especificar Servicios de AWS adicionales de los que desea recoger pruebas. Tras añadir estos servicios, las pruebas estarán disponibles al cabo de 24 horas.

> **Note**
>
> Si ha creado la evaluación a partir de un marco estándar, la lista de Servicios de AWS incluidos en el ámbito de aplicación está preseleccionada y no se puede editar. Esto se debe a que cuando crea una evaluación a partir de un marco estándar, Audit Manager asigna y selecciona automáticamente el origen de datos y los servicios relevantes para usted. La selección se realiza en función de los requisitos del marco estándar. Tenga en cuenta que, en el caso de los marcos estándar que solo contienen controles manuales, ningún Servicios de AWS está incluido.
>
> La solución alternativa para editar el Servicios de AWS incuido y, al mismo tiempo, crear una evaluación basada en un marco estándar consiste en personalizar el marco estándar. Al utilizar esta solución alternativa, puede utilizar el marco que ha personalizado para crear una nueva evaluación. En esta evaluación, puede especificar cuáles Servicios de AWS están incluidos.

Mis pruebas se generan a intervalos diferentes y no estoy seguro de la frecuencia con la que se recopilan

Los controles de las evaluaciones de Audit Manager se asignan a varios orígenes de datos. Cada origen de datos tiene una frecuencia de recopilación de evidencias diferente. Como resultado, no existe una respuesta única para la frecuencia con la que se recopilan las pruebas. Algunas fuentes de datos evalúan el cumplimiento, mientras que otras solo recopilan el estado de los recursos y modifican los datos sin determinar el cumplimiento.

El siguiente es un resumen de los distintos tipos orígenes de datos y de la frecuencia con la que recopilan pruebas.

Data source type	Descripción	Frecuencia de recolección de evidencia	Cuando este control está activo en una evaluación
AWS CloudTrail	Realiza un seguimiento de la actividad de un usuario específico.	Continuo	Audit Manager filtra los registros de CloudTrail en función de la palabra clave que elija. Los registros procesados se importan como evidencia de la Actividad del usuario.
AWS Security Hub	Captura una instantánea del estado de seguridad de sus recursos mediante el informe de los resultados de Security Hub.	Según la programación de la comprobación del Security Hub (normalmente cada 12 horas)	Audit Manager recupera los resultados de seguridad directamente desde Security Hub. El resultado se importa como prueba de Control de conformidad.
AWS Config	Captura una instantánea del estado de seguridad de sus recursos mediante un informe de los resultados obtenidos de AWS Config.	En función de la configuración definida en la regla AWS Config	Audit Manager recupera la evaluación de la regla directamente de AWS Config. La evaluación se importa como evidencia de Control de conformidad.
AWSLlamadas a la API	Toma una instantánea de la configuración de sus recursos directame	Diariamente, semanalmente o	Audit Manager realiza la llamada a la API en función de la frecuencia que especifique. La respuesta se importa como evidencia de Datos de configuración.

Data source type	Descripción	Frecuencia de recolección de evidencia	Cuando este control está activo en una evaluación
	nte mediante una llamada a la API especificada Servicio de AWS.	mensualmente	

Independientemente de la frecuencia de recopilación de evidencias, las nuevas evidencias se recopilan automáticamente mientras la evaluación esté activa. Para obtener más información, consulte Frecuencia de recopilación de evidencias.

Para obtener más información, consulte Origen de datos de control compatibles para pruebas automatizadas y Cambiar la frecuencia de recopilación de evidencias para un control.

¿Qué ocurre si elimino una cuenta incluida en el ámbito de aplicación de mi organización?

Cuando se elimina una cuenta incluida en el ámbito de su organización, Audit Manager deja de recopilar pruebas de esa cuenta. Sin embargo, la cuenta sigue apareciendo en su evaluación, en la pestaña Cuentas de AWS. Para eliminar la cuenta de la lista de cuentas incluidas, edite la evaluación. La cuenta eliminada ya no aparece en la lista durante la edición y puede guardar los cambios sin esa cuenta incluida.

No puedo editar los servicios incluidos en el ámbito de mi evaluación

Al utilizar la consola Audit Manager para crear una evaluación a partir de un marco estándar, la lista de dentro de Servicios de AWS incluida se selecciona de forma predeterminada. Esta lista no se puede editar. Esto se debe a que Audit Manager asigna y selecciona automáticamente el origen de datos y los servicios por usted. Esta selección se realiza de acuerdo con los requisitos del marco estándar. Si el marco estándar que ha seleccionado contiene solo controles manuales, ningún Servicios de AWS está incluido en el ámbito de su evaluación y no puede añadir ningún servicio a su evaluación.

Si necesita editar la lista de servicios incluidos, utilice la operación de API UpdateAssessment proporcionada por Audit Manager. Como alternativa, puede personalizar el marco estándar y, a continuación, crear una evaluación a partir del marco personalizado.

¿Cuál es la diferencia entre un servicio incluido y un tipo de origen de datos?

Un servicio incluido es aquel Servicio de AWS que se especifica como parte de su evaluación. Cuando un servicio está incluido, Audit Manager recopila evidencia sobre el uso que usted hace de ese servicio y sus recursos.

Un tipo de origen de datos indica de dónde se recopilan exactamente las pruebas. Si carga sus propias evidencias, el tipo de origen de datos es Manual. Si Audit Manager recopila evidencias, el origen de datos puede ser de cuatro tipos.

1. AWS Security Hub: captura una instantánea del estado de seguridad de sus recursos mediante el informe de los resultados de Security Hub.
2. AWS Config: captura una instantánea del estado de seguridad de sus recursos mediante un informe de los resultados obtenidos de AWS Config.
3. AWS CloudTrail: realiza un seguimiento de la actividad de un usuario específico en relación con un recurso.
4. Llamadas a la API de AWS: toma una instantánea de la configuración de los recursos directamente a través de una llamada a la API a una Servicio de AWS específica.

Estos son dos ejemplos para ilustrar la diferencia entre el alcance de un servicio y el tipo de origen de datos.

Ejemplo 1

Supongamos que desea recopilar pruebas para un control denominado 4.1.2: no permitir el acceso de escritura pública a los buckets de S3. Este control comprueba los niveles de acceso de sus políticas de bucket de S3. Para este control, Audit Manager utiliza una regla AWS Config específica (s3-bucket-public-write-prohibited) para buscar una evaluación de sus buckets de S3. En este ejemplo, se aplica lo siguiente:

- El servicio incluido es Amazon S3
- Los recursos que se están evaluando son sus buckets de S3

- El tipo del origen de datos es AWS Config
- La asignación de origen de datos es una AWS Config regla específica (`s3-bucket-public-write-prohibited`)

Ejemplo 2

Supongamos que desea recopilar pruebas para un control de la HIPAA denominado 164.308(a)(5)(ii)(C). Este control requiere un procedimiento de supervisión para detectar inicios de sesión inadecuados. Para este control, Audit Manager utiliza los registros de CloudTrail para buscar todos los eventos de inicio de sesión de la Consola de administración de AWS. Esto se muestra en el siguiente ejemplo:

- El servicio incluido es IAM
- Los recursos que se están evaluando son sus usuarios
- El tipo de origen de datos es CloudTrail
- La asignación de origen de datos es un evento de CloudTrail específico (`ConsoleLogin`)

Error al crear mi evaluación

Si la creación de la evaluación falla, podría deberse a que seleccionó demasiadas Cuentas de AWS en el ámbito de la evaluación. Si utiliza AWS Organizations, Audit Manager puede admitir hasta aproximadamente 150 cuentas de miembros en el ámbito de una sola evaluación. Si supera este número, es posible que se produzca un error durante la creación de la evaluación. Como solución alternativa, puede ejecutar varias evaluaciones con diferentes cuentas para cada evaluación.

He desactivado Audit Manager y, a continuación, he vuelto a activarlo, y ahora mis evaluaciones preexistentes ya no recopilan pruebas

Cuando desactiva Audit Manager y decide no eliminar sus datos, las evaluaciones existentes pasan a un estado latente y dejan de recopilar pruebas. Esto significa que cuando vuelva a activar Audit Manager, las evaluaciones que creó anteriormente permanecerán disponibles. Sin embargo, no reanudan automáticamente la recopilación de pruebas.

Para volver a recopilar evidencias para una evaluación preexistente, edite la evaluación y seleccione Guardar sin realizar ningún cambio.

Solución de problemas con el informe de evaluación

Puede utilizar la información de esta página para resolver problemas comunes de los informes de evaluación en Audit Manager.

Temas

No se pudo generar mi informe de evaluación

Es posible que el informe de evaluación no se haya generado por varias razones. Puede empezar a solucionar este problema comprobando las causas más frecuentes. Use la siguiente lista de verificación para empezar.

1. Comprueba si alguno de sus datos Región de AWS no coincide:
   a. ¿La Región de AWS de la clave gestionada por el cliente coincide con la Región de AWS de su evaluación?

      Si proporcionó su propia clave KMS para el cifrado de datos de Audit Manager, la clave debe estar en la misma Región de AWS que la de su evaluación. Para resolver este problema, cambie la clave KMS por una que esté en la misma Región que la evaluación. Para obtener instrucciones sobre cómo cambiar la clave KMS, consulte AWS Audit ManagerConfiguración y cifrado de datos.
   b. ¿La Región de AWS de la clave gestionada por el cliente coincide con la Región de AWS de su evaluación?

      Si proporcionó su propia clave KMS para el cifrado de datos de Audit Manager, la clave debe estar en la misma Región de AWS que el bucket de S3 que utiliza como destino del informe

de evaluación. Para resolver este problema, puede cambiar la clave KMS o el bucket de S3 para que ambos estén en la misma región que la evaluación. Para obtener instrucciones sobre cómo cambiar la clave KMS, consulte AWS Audit ManagerConfiguración y cifrado de datos. Para obtener instrucciones sobre cómo cambiar el bucket de S3, consulte AWS Audit ManagerConfiguración y destino del informe de evaluación.

2. Compruebe los permisos del bucket de S3 que está utilizando como destino del informe de evaluación:

   a. ¿La entidad de IAM que genera el informe de evaluación tiene los permisos necesarios para el bucket de S3?

      La entidad de IAM debe tener los permisos del bucket de S3 necesarios para publicar los informes en ese bucket. Proporcionamos un ejemplo de política que puede utilizar. Para obtener instrucciones sobre cómo especificar un bucket de S3 diferente, consulte AWS Audit ManagerConfiguración y destino del informe de evaluación.

   b. ¿El bucket de S3 tiene una política de bucket que requiera el cifrado del servidor (SSE) mediante SSE-KMS?

      En caso afirmativo, la clave de KMS que se utiliza en esa política de bucket debe coincidir con la clave de KMS que se especifica en la configuración de cifrado de datos de Audit Manager. Si no configuró una clave KMS en la configuración de Audit Manager y su política de bucket de S3 requiere SSE, asegúrese de que la política de bucket permita SSE-S3. Para obtener instrucciones sobre cómo cambiar la clave KMS, consulte AWS Audit ManagerConfiguración y cifrado de datos. Para obtener instrucciones sobre cómo cambiar el bucket de S3, consulte AWS Audit ManagerConfiguración y destino del informe de evaluación.

Si sigue sin poder generar correctamente un informe de evaluación, revise los siguientes problemas en esta página.

He seguido la lista de verificación anterior y mi informe de evaluación sigue sin generarse

Audit Manager limita la cantidad de evidencia que se puede añadir a un informe de evaluación. El límite se basa en Región de AWS de su evaluación, en la región del bucket de S3 que se utiliza como destino del informe de evaluación y en si la evaluación utiliza una evaluación gestionada por el cliente AWS KMS key.

1. El límite es de 22.000 para los informes de la misma región (en los que el bucket de S3 y la evaluación están en la misma Región de AWS)
2. El límite es de 3500 para los informes de la misma región (en los que el bucket de S3 y la evaluación están en la misma Regiones de AWS)
3. El límite es de 3500 si la evaluación utiliza una clave KMS administrada por el cliente

Si intenta generar un informe que contenga más pruebas que estas, la operación podría fallar.

Como solución alternativa, puede generar varios informes de evaluación en lugar de un informe de evaluación más grande. De este modo, puede exportar las pruebas de su evaluación a lotes de un tamaño más manejable.

Cuando intento generar un informe, aparece un error de acceso denegado

Aparecerá un error `access denied` si la evaluación la creó una cuenta de administrador delegado a la que no pertenece la clave KMS especificada en la configuración de Audit Manager. Para evitar este error, cuando designe un administrador delegado para Audit Manager, asegúrese de que la cuenta de administrador delegado tenga acceso a la clave KMS que proporcionó al configurar Audit Manager.

También puede recibir un error `access denied` si no tiene permisos de escritura para el bucket de S3 que utiliza como destino del informe de evaluación.

Si aparece un error `access denied`, asegúrese de cumplir los siguientes requisitos:

- La clave KMS en la configuración de Audit Manager otorga permisos al administrador delegado. Para configurarlo, siga las instrucciones de la Guía para AWS Key Management Service desarrolladores sobre cómo permitir que los usuarios de otras cuentas usen una clave KMS. Para obtener instrucciones sobre cómo revisar y cambiar la configuración de cifrado en Audit Manager, consulte Cifrado de datos.
- Tiene una política de permisos que le otorga acceso de escritura al bucket de S3 que utiliza como destino del informe de evaluación. Más específicamente, su política de permisos contiene una acción `s3:PutObject`, especifica el ARN del bucket de S3 e incluye la clave KMS que se utiliza para cifrar los informes de evaluación. Para ver un ejemplo de política que pueda usar, consulte los ejemplos de políticas basadas en la identidad para AWS Audit Manager.

> **Note**
>
> Al cambiar la configuración de cifrado de datos de Audit Manager, estos cambios se aplican a cualquier evaluación nueva que cree. Esto incluye todos los informes de evaluación que cree a partir de sus nuevas evaluaciones.
> Los cambios no se aplican a las evaluaciones existentes que creó antes de cambiar la configuración del cifrado. Esto incluye los nuevos informes de evaluación que se crean a partir de las evaluaciones existentes, además de los informes de evaluación existentes. Las evaluaciones existentes (y todos sus informes de evaluación) siguen utilizando la antigua clave KMS. Si la identidad de IAM que genera el informe de evaluación no tiene permisos para usar la antigua clave de KMS, puede conceder permisos a nivel de política clave.

No puedo abrir el informe de evaluación

Si no puede descomprimir el informe de evaluación en Windows, es probable que el Explorador de Windows no pueda extraerlo porque la ruta del archivo tiene varias carpetas anidadas o nombres largos. Esto se debe a que, según el sistema de nombres de archivos de Windows, la ruta de la carpeta, el nombre y la extensión del archivo no pueden superar los 259 caracteres. De lo contrario, se produce un error `Destination Path Too Long`.

Para resolver este problema, intente mover el archivo zip a la carpeta principal de su ubicación actual. A continuación, puede volver a intentar descomprimirlo desde allí. Como alternativa, también puede intentar acortar el nombre del archivo zip o extraerlo a una ubicación diferente que tenga una ruta de archivo más corta.

Cuando elijo el nombre de una prueba en un informe, no se me redirige a los detalles de la evidencia

Este problema puede producirse si está interactuando con el informe de evaluación en un navegador o si utiliza el lector de PDF predeterminado que viene instalado en su sistema operativo. Algunos lectores de PDF predeterminados del navegador y del sistema no permiten abrir los enlaces correspondientes. Esto significa que, si bien los hipervínculos pueden funcionar dentro del PDF con el resumen del informe de evaluación (como los nombres de los controles con hipervínculos en el índice), los hipervínculos se ignoran cuando se intenta pasar del PDF con el resumen de la evaluación a otro PDF con detalles probatorios.

Si se produce este problema, le recomendamos que utilice un lector de PDF específico para interactuar con los informes de evaluación. Para disfrutar de una experiencia fiable, le recomendamos que instale y utilice Adobe Acrobat Reader, que puede descargar en el sitio web de Adobe. También hay otros lectores de PDF disponibles, pero se ha demostrado que Adobe Acrobat Reader funciona de forma coherente y fiable con los informes de evaluación de Audit Manager.

La generación de mi informe de evaluación está bloqueada en el estado En curso y no estoy seguro de cómo afecta esto a mi facturación

La generación de los informes de evaluación no afecta a la facturación. Solo se le facturará en función de la evidencia que recopilen sus evaluaciones. Para obtener más información sobre los precios, consulte Precios de AWS Audit Manager.

Véase también

Las siguientes páginas contienen una guía de solución de problemas sobre la generación de un informe de evaluación a partir del buscador de evidencias:

- No puedo generar varios informes de evaluación a partir de los resultados de mi búsqueda
- No puedo añadir resultados de búsqueda individuales a un informe de evaluación
- No todos los resultados de mi buscador de evidencias se incluyen en el informe de evaluación
- Quiero generar un informe de evaluación a partir de los resultados de mi búsqueda, pero el enunciado de mi consulta no funciona

Solución de problemas de control y conjunto de control

Puede utilizar la información de esta página para resolver problemas comunes con los controles de Audit Manager.

Problemas generales

- No veo ningún control o conjunto de controles en mi evaluación
- No puedo subir pruebas manuales a un control

Problema de integración de AWS Config

- Necesito usar varias reglas AWS Config como origen de datos para un solo control

- La opción de regla personalizada no está disponible cuando configuro un origen de datos de control
- La opción de regla personalizada está disponible, pero no aparece ninguna regla en la lista desplegable
- Hay algunas reglas personalizadas disponibles, pero no puedo ver la regla que quiero usar
- No veo la regla administrada que quiero usar
- Quiero compartir un marco personalizado, pero tiene controles que utilizan reglas AWS Config personalizadas como origen de datos. ¿Puede el destinatario recopilar pruebas para estos controles?
- ¿Qué ocurre cuando se actualiza una regla personalizada en AWS Config? ¿Tengo que tomar alguna medida en Audit Manager?

No veo ningún control o conjunto de controles en mi evaluación

En resumen, para ver los controles de una evaluación, debe especificarse como propietario de la auditoría de esa evaluación. Además, necesita los permisos de IAM necesarios para ver y gestionar los recursos de Audit Manager relacionados.

Si necesita acceder a los controles de una evaluación, pida a uno de los propietarios de la auditoría de esa evaluación que lo especifique como propietario de la auditoría. Puede especificar los propietarios de la auditoría al crear o editar una evaluación.

Asegúrese también de que el usuario cuente con los permisos necesarios para administrar la evaluación. Recomendamos que los propietarios de la auditoría utilicen la política AWSAuditManagerAdministratorAccess. Si necesita ayuda con los permisos de IAM, póngase en contacto con su administrador o con AWSSoporte. Para obtener información sobre cómo añadir una política de IAM a un usuario, consulte Adición de permisos a un usuario y Adición y eliminación de permisos de identidad de IAM en la Guía del usuario de IAM.

No puedo subir pruebas manuales a un control

Si no puede cargar pruebas manualmente en un control, es probable que se deba a que el control está inactivo.

Para cargar pruebas manuales en un control, primero debe cambiar el estado del control a En revisión o Revisado. Para obtener más información, consulte Actualización del estado de control.

> **Important**
>
> Cada cuenta de Cuenta de AWS solo puede cargar manualmente hasta 100 archivos de pruebas a un control cada día. Si se supera esta cuota diaria, no se podrá realizar ninguna carga manual adicional en ese control. Si necesita cargar una gran cantidad de evidencias manuales en un solo control, hágalo en lotes durante varios días.

Necesito usar varias reglas AWS Config como origen de datos para un solo control

Puede usar una combinación de reglas administradas y reglas personalizadas para un solo control. Para ello, configure varios orígenes de datos para el control y seleccione el tipo de regla que prefiera para cada una de ellas. Puede definir hasta 10 orígenes datos para un único control personalizado.

La opción de regla personalizada no está disponible cuando configuro un origen de datos de control

Por lo tanto, usted no tiene permisos para ver las reglas personalizadas de su Cuenta de AWS o organización. Más específicamente, no tiene permisos para realizar la operación DescribeConfigrules en la consola de Audit Manager.

Para resolver este problema, póngase en contacto con el administrador AWS para recibir ayuda. Si es AWS administrador, puede proporcionar permisos a sus usuarios o grupos gestionando sus políticas de IAM.

La opción de regla personalizada está disponible, pero no aparece ninguna regla en la lista desplegable

Esto significa que no hay reglas personalizadas habilitadas ni disponibles para su uso en su Cuenta de AWS u organización.

Si aún no dispone de reglas personalizadasAWS Config, puede crear una. Para obtener instrucciones, consulte AWS Configreglas personalizadas en Guía de desarrolladores de AWS Config.

Si espera ver una regla personalizada, consulte el siguiente elemento de solución de problemas.

Hay algunas reglas personalizadas disponibles, pero no puedo ver la regla que quiero usar

Si no ve la regla personalizada que esperas encontrar, puede deberse a uno de los siguientes problemas.

Su cuenta está excluida de la regla

Es posible que la cuenta de administrador delegado que está utilizando esté excluida de la regla.

La cuenta de administración de su organización (o una de las cuentas de administrador AWS Config delegado) puede crear reglas organizativas personalizadas mediante AWS Command Line Interface (AWS CLI). Cuando lo hacen, pueden especificar una lista de cuentas que se van a excluir de la regla. Si su cuenta está en esta lista, la regla no está disponible en Audit Manager.

Para resolver este problema, póngase en contacto con el administrador AWS Config para recibir ayuda. Si es administrador AWS Config, puede actualizar la lista de cuentas excluidas ejecutando el comando put-organization-config-rule.

La regla no se creó y activó correctamente en AWS Config

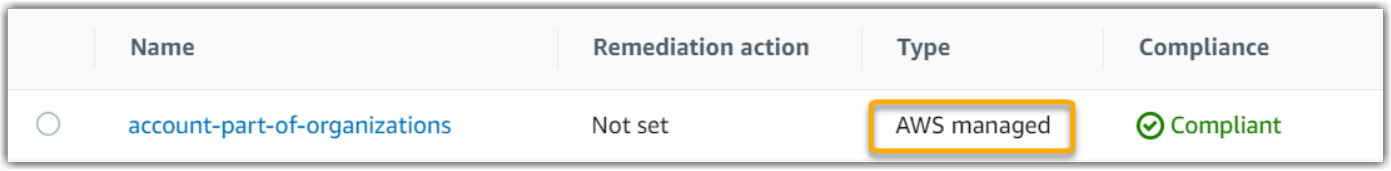
También es posible que la regla personalizada no se haya creado y activado correctamente. Si se ha producido un error al crear la regla, o la regla no está habilitada, no aparecerá en la lista de reglas disponibles en Audit Manager.

Para obtener ayuda con este problema, le recomendamos que se ponga en contacto con su AWS Config administrador.

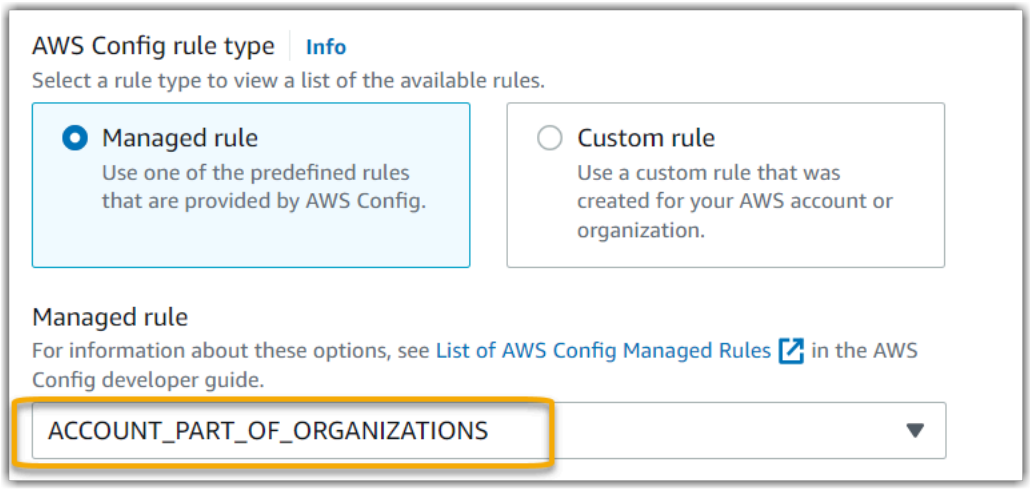
La regla es una regla administrada

Si no encuentra la regla que busca en la lista desplegable de reglas personalizadas, es posible que se trate de una regla administrada.

Puede usar la AWS Configconsola para comprobar si una regla es una regla administrada. Para ello, elija Reglas en el menú de navegación de la izquierda y busque la regla en la tabla. Si la regla es una regla administrada, la columna Tipo muestra la regla AWSadministrada.

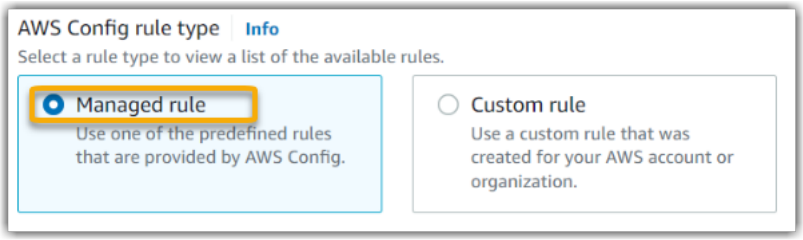


Una vez que haya confirmado que se trata de una regla administrada, vuelva a Audit Manager y seleccione Regla administrada como tipo de regla. A continuación, busque la palabra clave identificadora de la regla administrada en la lista desplegable de reglas administradas.



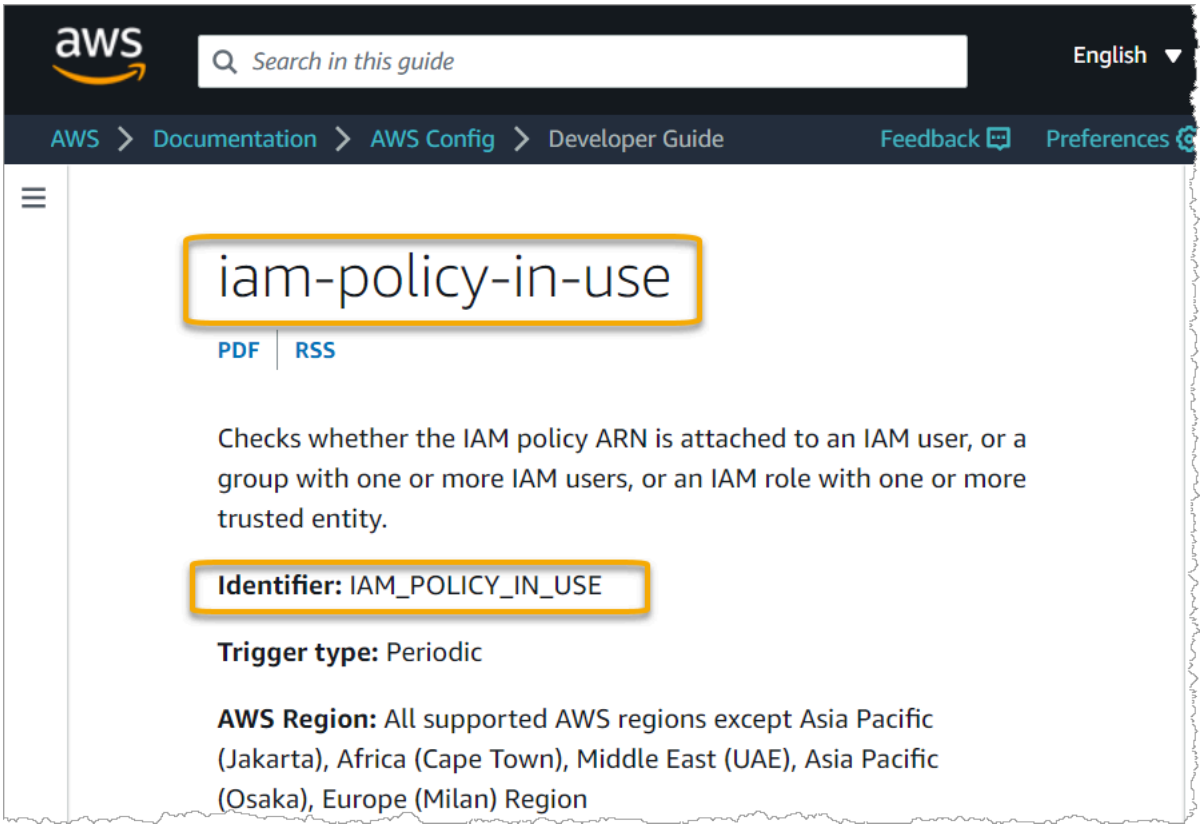
No veo la regla administrada que quiero usar

Antes de seleccionar una regla de la lista desplegable de la consola de Audit Manager, asegúrese de haber seleccionado Regla administrada como tipo de regla.

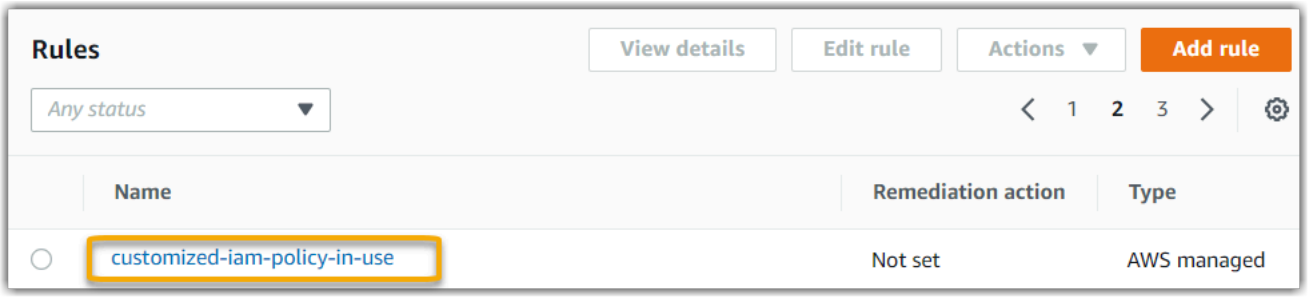


Si sigue sin ver la regla administrada que espera encontrar, es posible que esté buscando el nombre de la regla. En su lugar, debe buscar el identificador de la regla.

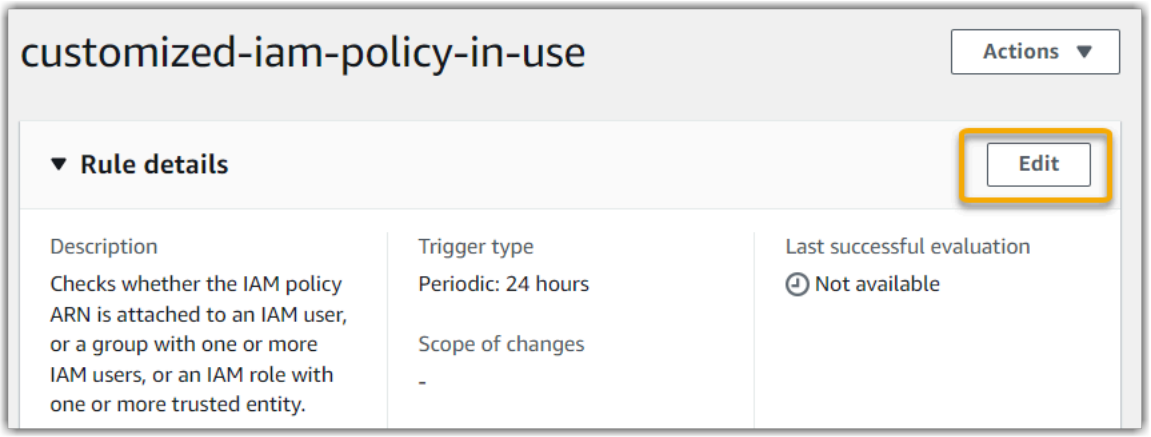
Si utiliza una regla administrada por defecto, el nombre y el identificador son similares. El nombre está en minúsculas y usa guiones (por ejemplo, `iam-policy-in-use`). El identificador está en mayúsculas y utiliza guiones bajos (por ejemplo, `IAM_POLICY_IN_USE`). Para encontrar el identificador de una regla administrada predeterminada, revise la lista de palabras clave de reglas AWS Config administradas compatibles y siga el enlace de la regla que desee usar. Esto le llevará a la documentación AWS Config de esa regla administrada. Desde aquí, puede ver tanto el nombre como el identificador. Busque la palabra clave del identificador en la lista desplegable de Audit Manager.



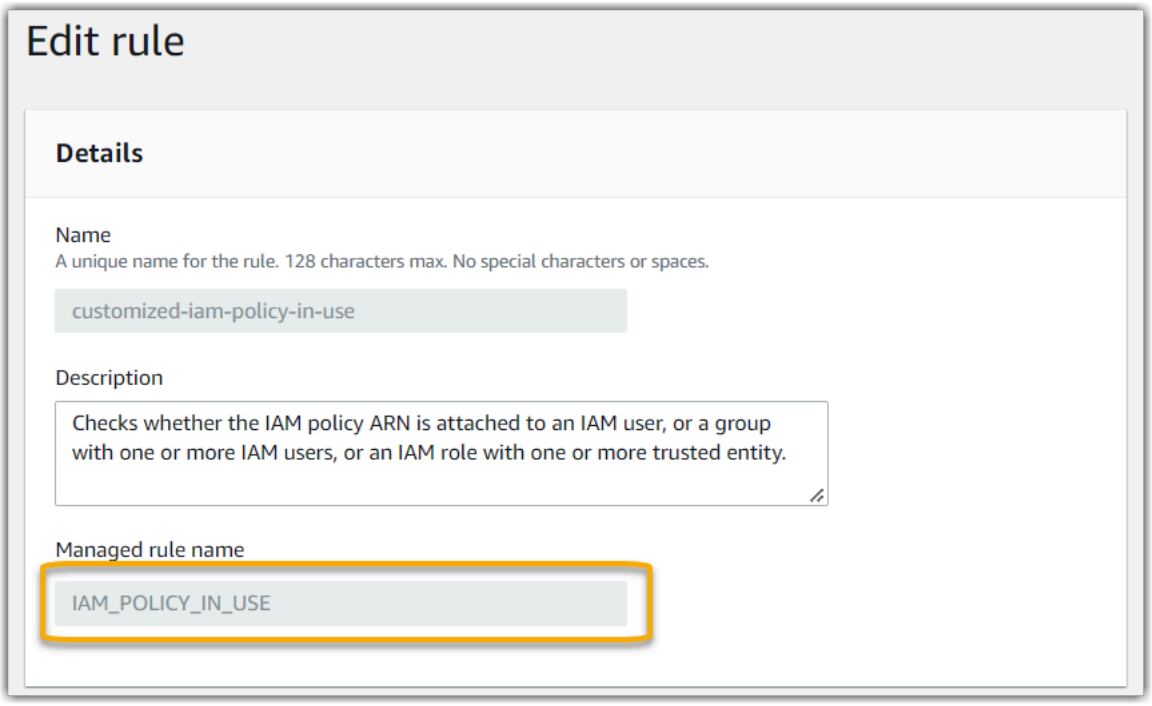
Si utiliza una regla administrada personalizada, puede usar la AWS Configconsola para buscar el identificador de la regla. Por ejemplo, supongamos que desea utilizar la regla administrada llamada `customized-iam-policy-in-use`. Para encontrar el identificador de esta regla, vaya a la AWS Config consola, elija Reglas en el menú de navegación de la izquierda y elija la regla en la tabla.



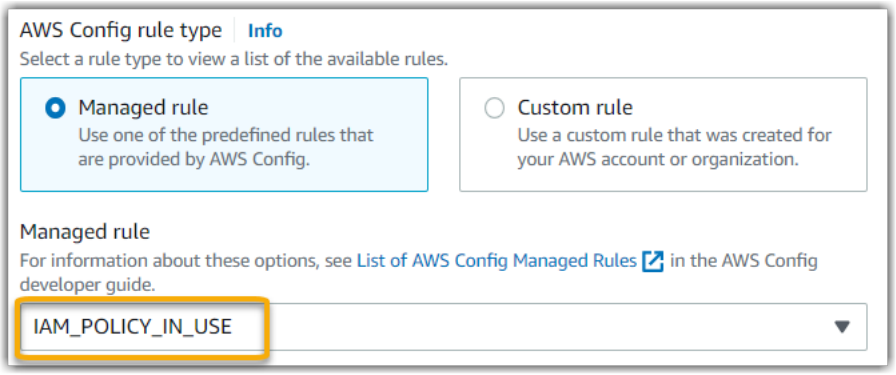
Elija Editar para abrir los detalles sobre la regla administrada.



En la sección Detalles, puede encontrar el identificador de origen a partir del cual se creó la regla administrada (`IAM_POLICY_IN_USE`).



Ahora puede volver a la consola de Audit Manager y seleccionar la misma palabra clave identificadora en la lista desplegable.



Quiero compartir un marco personalizado, pero tiene controles que utilizan reglas AWS Config personalizadas como origen de datos. ¿Puede el destinatario recopilar pruebas para estos controles?

Sí, el destinatario puede recopilar pruebas para estos controles, pero se necesitan algunos pasos para lograrlo.

Para que Audit Manager recopile pruebas utilizando una regla AWS Config como asignación de origen de datos, debe cumplirse lo siguiente. Esto es cierto para las reglas administradas y las reglas personalizadas.

1. La regla debe existir en el entorno AWS del destinatario
2. La regla debe estar habilitada en el entorno AWS del destinatario

Recuerde que es probable que las reglas AWS Config personalizadas de su cuenta aún no existan en el entorno AWS del destinatario. Además, cuando el destinatario acepta la solicitud de compartición, Audit Manager no vuelve a crear ninguna de sus reglas personalizadas en su cuenta. Para que el destinatario pueda recopilar pruebas utilizando sus reglas personalizadas como asignación de origen de datos, debe crear las mismas reglas personalizadas en su instancia de AWS Config. Una vez que el destinatario crea y, a continuación, activa las reglas, Audit Manager puede recopilar pruebas de ese origen de datos.

Le recomendamos que se comunique con el destinatario para informarle si es necesario crear alguna regla personalizada en su instancia de AWS Config.

¿Qué ocurre cuando se actualiza una regla personalizada en AWS Config? ¿Tengo que tomar alguna medida en Audit Manager?

Para actualizaciones de reglas en su entorno AWS

Si actualiza una regla personalizada en su entorno AWS, no es necesario realizar ninguna acción en Audit Manager. Audit Manager detecta y gestiona las actualizaciones de reglas como se describe en la tabla siguiente. Audit Manager no le notifica cuando se detecta una actualización de reglas.

Escenario	¿Qué hace Audit Manager?	Qué necesita
Se actualiza una regla personalizada en su instancia de AWS Config.	Audit Manager sigue informando de las conclusiones de esa regla mediante la definición de regla actualizada.	No es necesario ninguna acción.
Se elimina una regla personalizada en su instancia de AWS Config.	Audit Manager deja de informar de los resultados de la regla eliminada.	No es necesario ninguna acción. Si lo desea, puede editar los controles personalizados que utilizaban la regla eliminada como asignación de origen de datos. Esto ayuda a limpiar la configuración de la origen de datos al eliminar la regla eliminada. De lo contrario, el nombre de la regla eliminada permanece como una asignación de origen de datos no utilizada.

Para actualizaciones de reglas fuera de su entorno AWS

Si se actualiza una regla personalizada fuera de su entorno AWS, Audit Manager no detectará la actualización de la regla. Esto es algo que debe tener en cuenta si utiliza marcos personalizados

compartidos. Esto se debe a que, en este escenario, el remitente y el destinatario trabajan cada uno en entornos AWS separados. En la tabla siguiente se indican las acciones recomendadas para este escenario.

Su función	Escenario	Acción recomendada
Sender	• Compartió un marco que utiliza reglas personalizadas como asignación de origen de datos. • Tras compartir el marco, actualizó o eliminó una de esas reglas en AWS Config.	Informe al destinatario acerca de su actualización. De esta forma, pueden aplicar la misma actualización y mantenerse sincronizados con la definición de regla más reciente.
Recipie	• Ha aceptado un marco compartido que utiliza reglas personalizadas como asignación de origen de datos. • Tras volver a crear las reglas personalizadas en su instancia de AWS Config, el remitente actualizó o eliminó una de esas reglas.	Actualice la regla correspondiente en su propia instancia de AWS Config.

Solución de problemas de panel

Puede utilizar la información de esta página para resolver problemas comunes del panel de control en Audit Manager.

Temas

- No hay ningún dato en mi panel
- La opción de descarga en formato CSV no está disponible
- No veo el archivo descargado cuando intento descargar un archivo CSV
- Falta un control o dominio de control específico en el panel de control
- La instantánea diaria muestra cantidades variables de evidencia cada día. ¿Es esto normal?

No hay ningún dato en mi panel

Si los números del widget de instantáneas diarias muestran un guión (-), esto indica que no hay datos disponibles. Debe tener al menos una evaluación activa para ver los datos en el panel de control. Para empezar, cree una evaluación. Tras un periodo de 24 horas, los datos de la evaluación comenzarán a aparecer en el panel de control.

> **Note**
>
> Si los números del widget de instantáneas diarias muestran un cero (0), esto indica que las evaluaciones activas (o la evaluación seleccionada) no contienen pruebas que no cumplan con los requisitos.

La opción de descarga en formato CSV no está disponible

Esta opción solo está disponible para evaluaciones individuales. Asegúrese de haber aplicado una the section called “Filtro de evaluación” al panel de control e inténtelo de nuevo. Recuerde que solo puede descargar un archivo CSV a la vez.

No veo el archivo descargado cuando intento descargar un archivo CSV

Si un dominio de control contiene una gran cantidad de controles, es posible que se produzca un breve retraso mientras Audit Manager genera el archivo CSV. Una vez generado el archivo, se descarga automáticamente.

Si sigue sin ver el archivo descargado, asegúrese de que la conexión a Internet funciona correctamente y de que utiliza la versión más reciente del navegador web. Además, compruebe su carpeta de descargas recientes. Los archivos se descargan en la ubicación predeterminada que determine el navegador. Si esto no resuelve el problema, intente descargar el archivo con otro navegador.

Falta un control o dominio de control específico en el panel de control

Es probable que esto signifique que sus evaluaciones activas (o una evaluación específica) no contienen datos relevantes para ese control o dominio de control.

Un dominio de control se muestra en el panel de control solo si se cumplen los dos criterios siguientes:

- Las evaluaciones activas (o la evaluación específica) contienen al menos un control relacionado con ese dominio
- Al menos un control de ese dominio recopiló pruebas en la fecha que aparece en la parte superior del panel

Un control se muestra dentro de un dominio solo si recopiló pruebas en la fecha que aparece en la parte superior del panel.

La instantánea diaria muestra cantidades variables de evidencia cada día. ¿Es esto normal?

No todas las pruebas se recopilan a diario. Los controles de las evaluaciones de Audit Manager se asignan a diferentes origenes de datos, y cada una puede tener un calendario de recopilación de pruebas diferente. Como resultado, se espera que la instantánea diaria muestre una cantidad variable de evidencia cada día. Para obtener más información sobre la frecuencia de recopilación de evidencias, consulte Cómo se AWS Audit Manager recopilan las evidencias.

Solución de problemas AWS Organizations y del administrador delegado

Puede utilizar la información de esta página para resolver los problemas habituales de los administradores delegados en Audit Manager.

Temas

- No puedo configurar Audit Manager con mi cuenta de administrador delegado
- Cuando creo una evaluación, no puedo ver las cuentas de mi organización en Cuentas incluidas
- Aparece un error de acceso denegado cuando intento generar un informe de evaluación con mi cuenta de administrador delegado
- ¿Qué ocurre en Audit Manager si desvinculo la cuenta de un miembro de mi organización?
- ¿Qué ocurre si vuelvo a vincular la cuenta de un miembro a mi organización?
- ¿Qué ocurre si migro la cuenta de un miembro de una organización a otra?

No puedo configurar Audit Manager con mi cuenta de administrador delegado

Aunque se admiten varios administradores delegados en AWS Organizations, Audit Manager solo permite un administrador delegado. Si intenta designar varios administradores delegados en Audit Manager, recibirá el siguiente mensaje de error como el que sigue:

- Consola: `You have exceeded the allowed number of delegated administrators for the delegated service`
- CLI: `An error occurred (ValidationException) when calling the RegisterAccount operation: Cannot change delegated Admin for an active account 11111111111 from 2222222222222 to 333333333333`

Elija la cuenta individual que desee usar como administrador delegado en Audit Manager. Asegúrese de registrar primero la cuenta de administrador delegado en Organizations y, a continuación, de añadir la misma cuenta que un administrador delegado en Audit Manager.

Cuando creo una evaluación, no puedo ver las cuentas de mi organización en Cuentas incluidas

Si desea que la evaluación de Audit Manager incluya varias cuentas de su organización, debe especificar un administrador delegado.

Asegúrese de configurar una cuenta de administrador delegado para Audit Manager. Para obtener instrucciones, consulte Configuración, administrador delegado.

Algunas cuestiones a tener en cuenta:

- No puede usar su cuenta de administración AWS Organizations como administrador delegado en Audit Manager.
- Si desea activar Audit Manager en más de una Región de AWS, debe designar una cuenta de administrador delegado por separado en cada región. En la configuración de Audit Manager, designe la misma cuenta de administrador delegado en todas las regiones.
- Cuando designe un administrador delegado, asegúrese de que la cuenta de administrador delegado tenga acceso a la clave de KMS que proporcionó al configurar Audit Manager. Para obtener información sobre cómo revisar y cambiar la configuración de cifrado, consulte Cifrado de datos.

Aparece un error de acceso denegado cuando intento generar un informe de evaluación con mi cuenta de administrador delegado

Aparecerá un error `access denied` si la evaluación la creó una cuenta de administrador delegado a la que no pertenece la clave KMS especificada en la configuración de Audit Manager. Para evitar este error, cuando designe un administrador delegado para Audit Manager, asegúrese de que la cuenta de administrador delegado tenga acceso a la clave KMS que proporcionó al configurar Audit Manager.

También puede recibir un error `access denied` si no tiene permisos de escritura para el bucket de S3 que utiliza como destino del informe de evaluación.

Si aparece un error `access denied`, asegúrese de cumplir los siguientes requisitos:

- La clave KMS en la configuración de Audit Manager otorga permisos al administrador delegado. Para configurarlo, siga las instrucciones de la AWS Key Management ServiceGuía para desarrolladores sobre cómo permitir que los usuarios de otras cuentas usen una clave KMS. Para obtener instrucciones sobre cómo revisar y cambiar la configuración de cifrado en Audit Manager, consulte Cifrado de datos.
- Tiene una política de permisos que le otorga acceso de escritura al destino del informe de evaluación. Más específicamente, su política de permisos contiene una acción `s3:PutObject`, especifica el ARN del bucket de S3 e incluye la clave KMS que se utiliza para cifrar los informes de evaluación. Para ver un ejemplo de política que pueda usar, consulte los ejemplos de políticas basadas en la identidad para AWS Audit Manager.

> **Note**
>
> Al cambiar la configuración de cifrado de datos de Audit Manager, estos cambios se aplican a cualquier evaluación nueva que cree. Esto incluye todos los informes de evaluación que cree a partir de sus nuevas evaluaciones.
> Los cambios no se aplican a las evaluaciones existentes que creó antes de cambiar la configuración del cifrado. Esto incluye los nuevos informes de evaluación que se crean a partir de las evaluaciones existentes, además de los informes de evaluación existentes. Las evaluaciones existentes (y todos sus informes de evaluación) siguen utilizando la antigua clave KMS. Si la identidad de IAM que genera el informe de evaluación no tiene permisos para usar la antigua clave de KMS, puede conceder permisos a nivel de política clave.

¿Qué ocurre en Audit Manager si desvinculo la cuenta de un miembro de mi organización?

Al desvincular la cuenta de un miembro de una organización, Audit Manager recibe una notificación sobre este evento. A continuación, Audit Manager elimina esa Cuenta de AWS automáticamente de las listas de cuentas incluidas de sus evaluaciones existentes. Al especificar el ámbito de las nuevas evaluaciones en el futuro, la cuenta desvinculada ya no aparece en la lista de Cuentas de AWS elegibles.

Cuando Audit Manager elimina una cuenta de miembro desvinculada de las listas de cuentas incluidas de sus evaluaciones, no se le notifica este cambio. Además, a la cuenta de miembro desvinculada no se le notifica que Audit Manager ya no está activado en su cuenta.

¿Qué ocurre si vuelvo a vincular la cuenta de un miembro a mi organización?

Cuando vuelve a vincular una cuenta de miembro a u organización, esa cuenta no se añade automáticamente al ámbito de sus evaluaciones de Audit Manager existentes. Sin embargo, la cuenta de miembro que se ha vuelto a vincular ahora aparece como elegible Cuenta de AWS al especificar las cuentas incluidas en el ámbito de sus evaluaciones.

- En el caso de las evaluaciones existentes, puede editar manualmente el ámbito de la evaluación para añadir la cuenta de miembro revinculada. Para obtener instrucciones, consulte Editar Cuentas de AWS incluido.
- Para las nuevas evaluaciones, puede añadir la cuenta revinculada durante la configuración de la evaluación. Para obtener instrucciones, consulte Especificar Cuentas de AWS incluido.

¿Qué ocurre si migro la cuenta de un miembro de una organización a otra?

Si la cuenta de un miembro tiene Audit Manager activado en la organización 1 y, a continuación, migra a la organización 2, Audit Manager no estará habilitado para la organización 2 como resultado.

Solución de problemas con el buscador de evidencias

Utilice la información de esta página para resolver problemas comunes relacionados con el buscador de evidencias en Audit Manager.

Problemas generales relacionados con el buscador de evidencias

- No puedo habilitar el buscador de evidencias
- He activado el buscador de evidencias, pero no veo pruebas anteriores en los resultados de mi búsqueda
- No puedo desactivar el buscador de evidencias
- Mi consulta de búsqueda falla

Problemas con el informe de evaluación del buscador de evidencias

- No puedo generar varios informes de evaluación a partir de los resultados de mi búsqueda
- No puedo incluir pruebas específicas de los resultados de mi búsqueda
- No todos los resultados de mi buscador de evidencias se incluyen en el informe de evaluación
- Quiero generar un informe de evaluación a partir de los resultados de mi búsqueda, pero el enunciado de mi consulta no funciona
- Más recursos

Problemas de exportación a CSV del del buscador de evidencias

- Mi exportación CSV ha fallado
- No puedo exportar pruebas específicas de los resultados de mi búsqueda
- No puedo exportar varios archivos CSV a la vez

No puedo habilitar el buscador de evidencias

Algunas razones comunes por las que no puede cerrar una incluyen las siguientes situaciones:

Le faltan permisos

> Si está intentando activar el buscador de evidencias por primera vez, asegúrese de tener los permisos necesarios. Estos permisos le permiten crear y administrar un almacén de datos de eventos en CloudTrail Lake, que es necesario para respaldar las consultas de búsqueda del buscador de evidencias. Los permisos también le permiten realizar consultas de búsqueda en el buscador de evidencias.

Si necesita ayuda con los permisos, póngase en contacto con su administrador de AWS. Si es un administrador AWS, puede copiar la declaración de permiso requerida y adjuntarla a una política de IAM.

Está utilizando la cuenta de administración de Organizations

Recuerde que no puede usar la cuenta de administración para habilitar el buscador de evidencias. Inicie sesión como la cuenta de administrador delegado e inténtelo de nuevo.

Ha desactivado anteriormente el buscador de evidencias

Actualmente, no se permite volver a habilitar el buscador de evidencias. Si anteriormente desactivó el buscador de evidencias, no podrá volver a habilitarlo.

He activado el buscador de evidencias, pero no veo pruebas anteriores en los resultados de mi búsqueda

Al activar el buscador de evidencias, todos los datos de las pruebas anteriores tardan hasta 7 días en estar disponibles.

Durante este período de 7 días, se rellena un almacén de datos de eventos con los datos probatorios de los últimos dos años. Esto significa que si utiliza el buscador de evidencias inmediatamente después de activarlo, no estarán disponibles todos los resultados hasta que haya completado el proceso de relleno.

Para obtener instrucciones sobre cómo comprobar el estado del relleno de datos, consulte Confirmación del estado del buscador de evidencias.

No puedo desactivar el buscador de evidencias

Esto podría deberse a una de las siguientes causas.

Le faltan permisos

Si está intentando deshabilitar el buscador de evidencias, asegúrese de que tiene los permisos necesarios. Estos permisos le permiten actualizar y eliminar un almacén de datos de eventos de CloudTrail Lake, lo que es necesario para deshabilitar el buscador de evidencias.

Si necesita ayuda, póngase en contacto con su administrador de AWS. Si es un administrador AWS, puede copiar la declaración de permiso requerida y adjuntarla a una política de IAM.

Todavía se está tramitando una solicitud para habilitar el buscador de evidencias

Cuando solicita habilitar el buscador de evidencias, creamos un almacén de datos de eventos para respaldar las consultas del buscador de evidencias. No puede deshabilitar el buscador de evidencias mientras se crea el almacén de datos del evento.

Para continuar, espere a que se cree el almacén de datos de eventos e inténtelo de nuevo. Para obtener más información, consulte Confirmación del estado del buscador de evidencias.

Ya ha solicitado desactivar el buscador de evidencias

Cuando solicita la desactivación del buscador de evidencias, eliminamos el almacén de datos de eventos que se utiliza para las consultas del buscador de evidencias. Si intenta volver a desactivar el buscador de evidencias mientras se elimina el almacén de datos de eventos, aparecerá un mensaje de error.

En este caso, no es necesario realizar ninguna acción. Espere a que se elimine el almacén de datos de eventos. Tan pronto como se complete, el buscador de evidencias se desactivará. Para obtener más información, consulte Confirmación del estado del buscador de evidencias.

Mi consulta de búsqueda falla

Una consulta de búsqueda fallida puede deberse a una de las siguientes razones.

Le faltan permisos

Compruebe que el usuario tiene los permisos necesarios para ejecutar consultas de búsqueda y acceder a los resultados de la búsqueda. En concreto, necesita permisos para las siguientes acciones de CloudTrail:

- StartQuery
- DescribeQuery
- CancelQuery
- GetQueryResults

Si necesita ayuda, póngase en contacto con su administrador de AWS. Si es un administrador AWS, puede copiar la declaración de permiso requerida y adjuntarla a una política de IAM.

Está ejecutando el número máximo de consultas

Puede ejecutar hasta 5 consultas a la vez. Si ejecuta el número máximo de consultas simultáneas, se producirá un error `MaxConcurrentQueriesException`. Si aparece este

mensaje de error, espere un minuto a que finalicen algunas consultas y, a continuación, vuelva a ejecutar la consulta.

La declaración de consulta contiene un error de validación

Si utiliza la API o la CLI para realizar la operación CloudTrail Lake StartQuery, asegúrese de que su `queryStatement` es válida. Si la declaración de consulta contiene errores de validación, una sintaxis incorrecta o palabras clave no compatibles, el resultado es un `InvalidQueryStatementException`.

Para obtener más información sobre cómo escribir una consulta, consulte Crear o editar una consulta en la AWS CloudTrailGuía del usuario.

Para ver ejemplos de sintaxis válida, revise los siguientes ejemplos de sentencias de consulta que se pueden utilizar para consultar un almacén de datos de eventos del Administrador de Auditoría.

Ejemplo 1: investigue las pruebas y su estado de conformidad

En este ejemplo, se buscan pruebas con cualquier estado de conformidad en todas las evaluaciones consideradas, dentro de un intervalo de fechas específico.

```
SELECT eventData.evidenceId, eventData.resourceArn,
 eventData.resourceComplianceCheck FROM $EDS_ID WHERE eventTime > '2022-11-02
 00:00:00.000' AND eventTime < '2022-11-03 00:00:00.000'
```

Ejemplo 2: determine las pruebas de incumplimiento de un control

En este ejemplo, se buscan todas las pruebas que no cumplen con las normas de un intervalo de fechas especificado para una evaluación y un control específicos.

```
SELECT * FROM $EDS_ID WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-
ff22gg44hh66' AND eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.resourceComplianceCheck IN
 ('NON_COMPLIANT','FAILED','WARNING') AND eventData.controlId IN ('aa11bb22-cc33-
dd44-ee55-ff66gg77hh88')
```

Ejemplo 3: cuente las pruebas por su nombre

En este ejemplo, se enumeran las pruebas totales de una evaluación en un intervalo de fechas específico, agrupadas por nombre y ordenadas por recuento de pruebas.

```
SELECT eventData.eventName as eventName, COUNT(*) as totalEvidence FROM  $EDS_ID
 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime
 > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' GROUP BY
 eventData.eventName ORDER BY totalEvidence DESC
```

Ejemplo 4: explore las pruebas por origen de datos y servicio

En este ejemplo, se buscan todas las pruebas de un intervalo de fechas especificado para un servicio y un origen de datos específicos.

```
SELECT * FROM $EDS_ID WHERE eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.service IN ('dynamodb') AND
 eventData.dataSource IN ('AWS API calls')
```

Ejemplo 5: Explore las pruebas de conformidad por origen de datos y dominio de control

En este ejemplo, se buscan pruebas de conformidad para dominios de control específicos, donde las pruebas provienen de un origen de datos que no es AWS Config.

```
 SELECT * FROM $EDS_ID WHERE eventData.resourceComplianceCheck IN
 ('PASSED','COMPLIANT') AND eventData.controlDomainName IN ('Logging and
 monitoring','Data security and privacy') AND eventData.dataSource NOT IN ('AWS
 Config')
```

Otras excepciones de API

La API StartQuery puede fallar por otros motivos. Para obtener una lista completa de los posibles errores y descripciones, consulte la referencia sobre errores de StartQuery en la referencia de la AWS CloudTrail API.

No puedo generar varios informes de evaluación a partir de los resultados de mi búsqueda

Este error se debe a que se ejecutan demasiadas consultas de CloudTrail Lake al mismo tiempo.

Este error puede producirse si agrupa los resultados de la búsqueda e intenta generar inmediatamente informes de evaluación para cada partida de los resultados agrupados. Cuando obtiene los resultados de la búsqueda y genera un informe de evaluación, cada acción invoca una

consulta. Solo puede ejecutar hasta 5 consultas a la vez. Si ejecuta el número máximo de consultas simultáneas, se mostrará un error `MaxConcurrentQueriesException`.

Para evitar este error, asegúrese de no generar demasiados informes de evaluación a la vez. Si ejecuta el número máximo de consultas simultáneas, se mostrará un error `MaxConcurrentQueriesException`. Si recibe este mensaje de error, espere unos minutos a que se completen los informes de evaluación en curso.

Puede comprobar el estado de los informes de evaluación desde la página del centro de descargas de la consola de Audit Manager. Una vez completados los informes, vuelva a los resultados agrupados en el buscador de evidencias. A continuación, podrá seguir obteniendo los resultados y generar un informe de evaluación para cada partida.

No puedo incluir pruebas específicas de los resultados de mi búsqueda

Todos los resultados de la búsqueda se incluyen en el informe de evaluación. No puede añadir filas individuales de forma selectiva a su conjunto de resultados de búsqueda.

Si solo quiere incluir resultados de búsqueda específicos en el informe de evaluación, le recomendamos que edite sus filtros de búsqueda actuales. De esta forma, puede restringir los resultados para centrarse únicamente en las pruebas que desee incluir en el informe.

No todos los resultados de mi buscador de evidencias se incluyen en el informe de evaluación

Al generar un informe de evaluación, hay límites en cuanto a la cantidad de evidencia que se puede añadir. El límite se basa en Región de AWS de su evaluación, en la región del bucket de S3 que se utiliza como destino del informe de evaluación y en si la evaluación utiliza una evaluación gestionada por el cliente AWS KMS key.

1. El límite es de 22.000 para los informes de la misma región (en los que el bucket de S3 y la evaluación están en la misma Región de AWS)
2. El límite es de 3500 para los informes de la misma región (en los que el bucket de S3 y la evaluación están en la misma Regiones de AWS)
3. El límite es de 3500 si la evaluación utiliza una clave KMS administrada por el cliente

Si supera este límite, el informe aún se crea. Sin embargo, Audit Manager agrega solo los primeros 3500 o 22.000 elementos de evidencia al informe.

Para evitar este problema, le recomendamos que edite los filtros de búsqueda actuales. De esta forma, puede reducir los resultados de la búsqueda segmentando una cantidad menor de pruebas. Si es necesario, puede repetir este método y generar varios informes de evaluación en lugar de un informe más grande.

Quiero generar un informe de evaluación a partir de los resultados de mi búsqueda, pero el enunciado de mi consulta no funciona

Si utiliza la API CreateAssessmentReport y su enunciado de consulta devuelve una excepción de validación, consulte la siguiente tabla para obtener instrucciones sobre cómo solucionarlo.

> **Note**
>
> Incluso si una declaración de consulta funciona en CloudTrail, es posible que la misma consulta no sea válida para la generación de informes de evaluación en Audit Manager. Esto se debe a algunas diferencias en la validación de consultas entre los dos servicios.

Cláusul	Problema	Solución	Notas
`SELECT`	La cláusula `SELECT` contiene un nombre de columna	Elimine la cláusula `SELECT` y sustitúyala por `SELECT eventJson .`	Solo se admite `SELECT eventJson .` Esta validación la gestiona Audit Manager.
`FROM`	La cláusula `FROM` contiene un ID de almacén de datos de eventos no válido o bien El ID del almacén de datos de eventos proporcionado no coincide con el ID del almacén de	Elimine la cláusula `FROM` y sustitúyala por `FROM` *`edsID`*, donde el valor de `edsID` coincide con el ID del almacén de datos de eventos que se especifica en la configuración de Audit Manager. Puede recuperar el ARN del almacén de datos de eventos desde la configuración de Audit Manager. Para obtener más	Esta validación la gestiona Audit Manager.

Cláusul	Problema	Solución	Notas
	datos de eventos en la configuración de su Audit Manager.	información, consulte GetProducts en la Referencia de la API de AWS Audit Manager.	
`GROUP BY`	Hay una cláusula `GROUP BY` en la consulta	Elimine la cláusula `GROUP BY`.	Esta validación la gestiona Audit Manager.
`HAVING`	Hay una cláusula `HAVING` en la consulta	Elimine la cláusula `HAVING`.	Esta validación la gestiona Audit Manager.
`LIMIT`	La cláusula `LIMIT` contiene un valor que supera el límite máximo permitido	Si la cláusula `LIMIT` existe, asegúrese de que su valor sea igual o inferior al límite máximo admitido: • Para los informes de la misma región, el límite es de 22.000 • Para los informes entre regiones, el límite es de 3500 • En el caso de los informes en los que la evaluación correspondiente utiliza un cliente gestionado AWS KMS key, el límite es de 3500	En la consola, no hay límite en cuanto al número de resultados de evidencias que se pueden devolver. Sin embargo, al generar un informe de evaluación, se aplica un límite a la cantidad de evidencias que se pueden incluir. Si no se proporciona ningún valor `LIMIT` en el enunciado de consulta, se aplican los límites máximos predeterminados. Esta validación la gestiona Audit Manager.
`ORDER BY`	La cláusula `ORDER BY` contiene funciones agregadas o alias que no están presentes en la cláusula `SELECT`	Asegúrese de que la cláusula `ORDER BY` no contenga ninguna condición mediante el uso de funciones agregadas o alias.	Esta validación la gestiona la API StartQuery de CloudTrail.

Cláusul	Problema	Solución	Notas
`WHERE`	La cláusula `WHERE` contiene más de una `assessmentId` o bien La cláusula `WHERE` contiene un `assessmentId` valor que no coincide con el `assessmentId` de su solicitud `createAssessmentReport` o bien La cláusula `WHERE` contiene un nombre de columna no compatible	Asegúrese de que solo se especifique un AssessmentID y de que coincida con el parámetro AssessmentID que especificó en la solicitud de API `createAssessmentReport` . Elimine los nombres de columna no admitidos.	Esta validación la gestiona la API StartQuery de CloudTrail.

Ejemplos

En los siguientes ejemplos, se muestra cómo puede utilizar el parámetro `queryStatement` al llamar a la operación CreateAssessmentReport. Antes de utilizar estas consultas, sustituya el *`texto del marcador de posición`* por sus `edsId` y valores `assessmentId`.

Ejemplo 1: crear un informe (se aplica el límite para la misma región)

En este ejemplo, se crea un informe que incluye los resultados de los buckets de S3 creados entre el 22 y el 23 de enero de 2022.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-01-22 00:00:00.000' AND
 eventTime < '2022-01-23 00:00:00.000' AND eventName='CreateBucket' LIMIT 22000
```

Ejemplo 2: crear un informe (se aplica un límite entre regiones)

En este ejemplo, se crea un informe que incluye todos los resultados del almacén de datos de eventos y la evaluación del evento especificados, sin especificar ningún intervalo de fechas.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 7000
```

Ejemplo 3: crear un informe (por debajo del límite predeterminado)

En este ejemplo, se crea un informe que incluye todos los resultados del almacén de datos de eventos y la evaluación del evento especificados, con un límite inferior al máximo predeterminado.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 2000
```

Más recursos

La siguiente página contiene una guía general para la solución de problemas relacionados con los informes de evaluación:

- Solución de problemas con el informe de evaluación

Mi exportación CSV ha fallado

La exportación de CSV puede fallar por varias razones. Puede solucionar este problema comprobando las causas más frecuentes.

Primero, asegúrese de que cumple los requisitos previos para usar la característica de exportación de CSV:

Ha activado correctamente el buscador de evidencias

> Si no ha activado el buscador de evidencias, no podrá ejecutar una consulta de búsqueda ni exportar los resultados de la búsqueda.

El relleno de su almacén de datos de eventos está completo

Si utiliza el buscador de evidencias inmediatamente después de activarlo y aún está rellenando las pruebas, es posible que algunos resultados no estén disponibles. Para comprobar el estado del relleno, consulte Confirmar el estado del buscador de evidencias.

La consulta de búsqueda se ha realizado correctamente

Audit Manager no puede exportar los resultados de una consulta fallida. Para solucionar problemas relacionados con una consulta fallida, consulte Mi consulta de búsqueda falla.

Una vez que haya confirmado que cumple los requisitos previos, utilice la siguiente lista de comprobación para comprobar si hay posibles problemas:

1. Verifique el estado de la consulta de búsqueda:
   a. ¿Se ha cancelado la consulta? El buscador de evidencias muestra resultados parciales que se hayan procesado antes de que se cancelara la consulta. Sin embargo, Audit Manager no exporta resultados parciales a su bucket de S3 ni al centro de descargas.
   b. ¿La consulta lleva ejecutándose más de una hora? Es posible que las consultas que se ejecuten durante más de una hora agoten el tiempo de espera. El buscador de evidencias muestra resultados parciales que se hayan procesado antes de que se agotara el tiempo de espera de la consulta. Sin embargo, Audit Manager no exporta resultados parciales. Para evitar que se agote el tiempo de espera, puede reducir la cantidad de pruebas escaneadas editando la consulta de búsqueda para especificar un intervalo más reducido.
2. Comprueba el nombre y el URI del bucket de S3 de destino de exportación:
   a. ¿Existe el bucket que ha especificado? Si ha introducido el URI de un bucket de forma manual, asegúrese de no haber escrito nada mal. Un error tipográfico o un URI incorrecto pueden provocar un error `RESOURCE_NOT_FOUND` cuando Audit Manager intente exportar el archivo CSV a Amazon S3.
3. Compruebe los permisos del bucket de S3 de destino de exportación:
   a. ¿Tiene permisos de escritura del bucket de S3? Debe disponer de acceso de escritura para el bucket de S3 que utilice como destino de exportación. Más específicamente, la política de permisos de IAM debe incluir una acción `s3:PutObject` y el ARN del bucket, y debe incluir CloudTrail como principal del servicio. Proporcionamos un ejemplo de política que puede utilizar. Para obtener instrucciones sobre cómo usar un bucket de S3 diferente, consulte Exportar la configuración de destino.
4. Comprueba si alguno de sus datos Región de AWS no coincide:

a. ¿La Región de AWS de la clave gestionada por el cliente coincide con la Región de AWS de su evaluación? Si proporcionó una clave gestionada por el cliente para el cifrado de datos, debe estar en la misma Región de AWS que la de su evaluación. Para obtener instrucciones sobre cómo cambiar la clave KMS, consulte Configuración de cifrado de datos.

5. Compruebe los permisos de su cuenta de administrador delegado:

a. ¿La clave gestionada por el cliente en la configuración de Audit Manager concede permisos a su administrador delegado? Si utiliza una cuenta de administrador delegado y especificó una clave administrada por el cliente para el cifrado de datos, asegúrese de que el administrador delegado tenga acceso a esa clave de KMS. Para obtener más información, consulte Permitir que los usuarios de otras cuentas utilicen una clave de KMS en la AWS Key Management ServiceGuía para desarrolladores. Para revisar y cambiar la configuración de cifrado en Audit Manager, consulte Configuración de cifrado de datos.

> **Note**
>
> Si cambia la configuración de cifrado de datos de Audit Manager, estos cambios se aplicarán a las nuevas evaluaciones que cree en el futuro. Esto incluye cualquier archivo CSV que exporte de sus nuevas evaluaciones.
> Los cambios no se aplican a las evaluaciones existentes que creó antes de cambiar la configuración del cifrado. Esto incluye las nuevas exportaciones a CSV de las evaluaciones existentes, además de las exportaciones a CSV existentes. Las evaluaciones existentes (y todas sus exportaciones a CSV) siguen utilizando la antigua clave KMS. Si la identidad de IAM que exporta el archivo CSV no tiene permisos para usar la clave KMS anterior, puedes conceder permisos a nivel de política clave.

No puedo exportar pruebas específicas de los resultados de mi búsqueda

Todos los resultados de la búsqueda se incluyen en los resultados.

Si quiere incluir solo pruebas específicas en el archivo CSV, le recomendamos que edite sus filtros de búsqueda actuales. De esta forma, puede restringir los resultados para centrarse únicamente en las pruebas que desee exportar.

No puedo exportar varios archivos CSV a la vez

Este error se debe a que se ejecutan demasiadas consultas de CloudTrail Lake al mismo tiempo.

Esto puede ocurrir si agrupa los resultados de la búsqueda e intenta exportar inmediatamente un archivo CSV para cada partida de los resultados agrupados. Al obtener los resultados de la búsqueda y exportar un archivo CSV, cada una de estas acciones invoca una consulta. Solo puede ejecutar hasta cinco consultas a la vez. Si ejecuta el número máximo de consultas simultáneas, se mostrará un error `MaxConcurrentQueriesException`.

Para evitar este error, asegúrese de no exportar demasiados archivos CSV a la vez.

Para resolver este error, espere a que se completen las exportaciones CSV en curso. La mayoría de las exportaciones tardan unos minutos. Sin embargo, si exporta una gran cantidad de datos, la exportación puede tardar hasta una hora en completarse. No dude en salir del buscador de evidencias mientras la exportación esté en curso.

Puede comprobar el estado de la exportación desde el centro de descargas de la consola Audit Manager. Cuando los archivos exportados estén listos, vuelva a los resultados agrupados en el buscador de evidencias. A continuación, podrá seguir obteniendo los resultados y exportar un archivo CSV para cada partida.

Solución de problemas de uso compartido de marcos

Puede utilizar la información de esta página para resolver problemas comunes de uso compartido de marcos en Audit Manager.

Temas

El estado de mi solicitud de compartir enviada aparece como Fallido

Si intenta compartir un marco personalizado y se produce un error en la operación, le recomendamos que compruebe lo siguiente:

1. Asegúrese de que Audit Manager esté activado en el Cuenta de AWS del destinatario y en la región especificada. Para ver una lista de las regiones AWS Audit Manager compatibles, consulte

AWS Audit Manager puntos de conexión y cuotas en la Referencia general de Amazon Web Services.

2. Asegúrese de haber introducido el ID correcto Cuenta de AWS al especificar la cuenta del destinatario.
3. Asegúrese de no haber especificado una cuenta AWS Organizations de administración como destinatario. Puede compartir un marco personalizado con un administrador delegado, pero si intenta compartir un marco personalizado con una cuenta de administración, la operación fallará.
4. Si utiliza una clave gestionada por el cliente para cifrar los datos de Audit Manager, asegúrese de que la clave KMS esté habilitada. Si la clave de KMS está deshabilitada e intenta compartir un marco personalizado, la operación no se realizará correctamente. Para obtener instrucciones sobre cómo habilitar una clave KMS deshabilitada, consulte Habilitar y deshabilitar claves en la AWS Key Management ServiceGuía para desarrolladores.

Mi solicitud de uso compartido tiene un punto azul al lado. ¿Qué significa esto?

Una notificación con un punto azul indica que una solicitud de compartición requiere tu atención.

Notificaciones con puntos azules para los remitentes

Aparece un punto de notificación azul junto a las solicitudes de uso compartido enviadas con el estado de a punto de vencer. Audit Manager muestra la notificación con un punto azul para que pueda recordar al destinatario que tome medidas con respecto a la solicitud de compartición antes de que caduque.

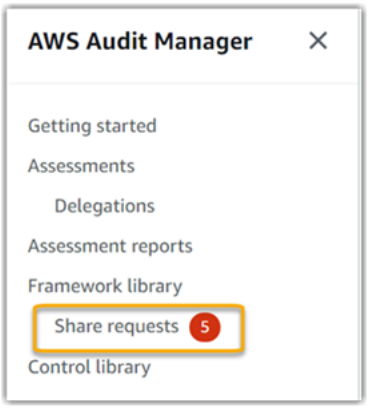
Para que desaparezca el punto azul de la notificación, el destinatario debe aceptar o rechazar la solicitud. El punto azul también desaparece si revoca la solicitud de compartir.

Puede usar el siguiente procedimiento para comprobar si hay solicitudes de uso compartido que estén venciendo y enviar un recordatorio opcional al destinatario para que tome las medidas oportunas.

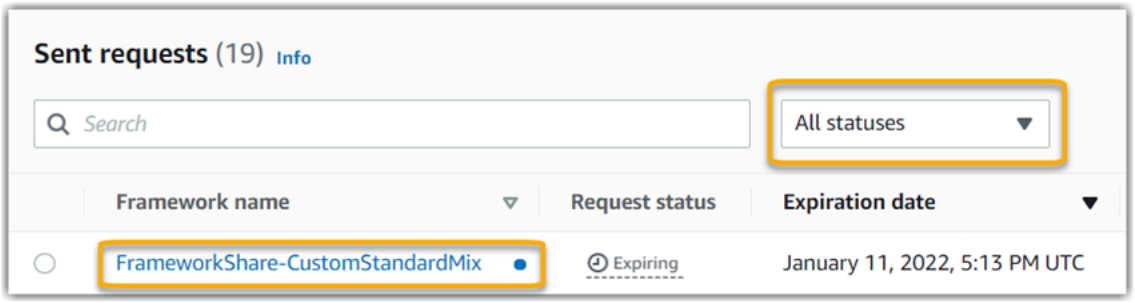
Para ver las notificaciones de las solicitudes enviadas

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home.
2. Si tiene una notificación de solicitud de uso compartido, Audit Manager muestra un punto rojo junto al icono del menú de navegación.

3. Despliegue el panel de navegación y busque junto a Solicitudes de uso compartido. Una insignia de notificación indica el número de solicitudes de uso compartido que requieren su atención.



4. Seleccione Compartir solicitudes y, a continuación, seleccione la pestaña Solicitudes enviadas.
5. Busque el punto azul para identificar las solicitudes de uso compartido que vencen en los próximos 30 días. Como alternativa, también puede ver las solicitudes de acciones que van a caducar seleccionando Vencimiento en el menú desplegable del filtro de todos los estados.



6. (Opcional) Recuerde al destinatario que debe tomar medidas con respecto a la solicitud de uso compartido antes de que caduque. Este paso es opcional, ya que Audit Manager envía una notificación a la consola para informar al destinatario cuando una solicitud de compartición está activa o va a caducar. Sin embargo, también puede enviar su propio recordatorio al destinatario a través del canal de comunicación que prefiera.

Notificaciones con puntos azules para los destinatarios

Junto a las solicitudes de uso compartido recibidas, aparece un punto de notificación azul con el estado Activo o A punto de vencer. Audit Manager muestra la notificación con un punto azul para recordarle que debe tomar medidas con respecto a la solicitud de participación antes de que venza.

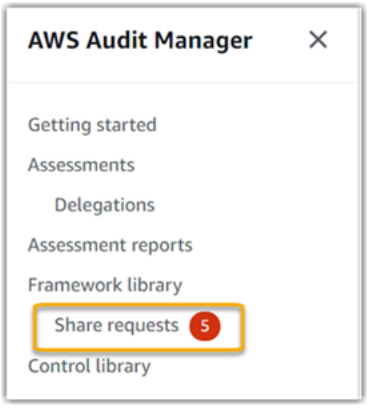
Para que desaparezca el punto azul de notificación, debe aceptar o rechazar la solicitud. El punto azul también desaparece si el remitente revoca la solicitud de compartir.

Puede utilizar el siguiente procedimiento para comprobar si hay solicitudes de uso compartido activas y vencidas.

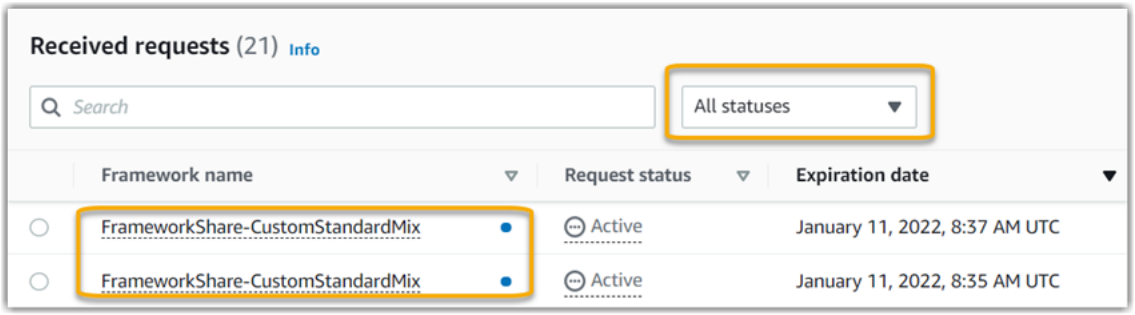
Para ver las notificaciones de las solicitudes recibidas

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/home..
2. Si tiene una notificación de solicitud de uso compartido, Audit Manager muestra un punto rojo junto al icono del menú de navegación.

3. Despliegue el panel de navegación y busque junto a Solicitudes de uso compartido. Una insignia de notificación indica el número de solicitudes de uso compartido que requieren tu atención.



4. Seleccione Solicitudes de uso compartido. De forma predeterminada, esta página se abre en la pestaña Solicitudes recibidas.
5. Busque los elementos con un punto azul para identificar las solicitudes de uso compartido que requieren su acción.



6. (Opcional) Para ver solo las solicitudes que vencen en los próximos 30 días, busque la lista desplegable Todos los estados y seleccione A punto de vencer.

Mi marco compartido tiene controles que utilizan reglas AWS Configpersonalizadas como origen de datos. ¿Puede el destinatario recopilar pruebas para estos controles?

Sí, su destinatario puede recopilar pruebas para estos controles, pero son necesarios algunos pasos para lograrlo.

Para que Audit Manager recopile pruebas utilizando una regla AWS Config como asignación de origen de datos, debe cumplirse lo siguiente. Estos criterios se aplican tanto a las reglas administradas como a las reglas personalizadas.

- La regla debe existir en el entorno del destinatario AWS.
- La regla debe estar habilitada en el entorno del destinatario AWS.

Recuerde que es probable que las reglas AWS Config de su cuenta aún no existan en el entorno del destinatario AWS. Además, cuando el destinatario acepta la solicitud de compartición, Audit Manager no vuelve a crear ninguna de sus reglas personalizadas en su cuenta. Para que el destinatario pueda recopilar pruebas utilizando sus reglas personalizadas como asignación de origen de datos, debe crear las mismas reglas personalizadas en su instancia de AWS Config. Una vez que el destinatario crea y, despuéshabilita las reglas en AWS Config, Audit Manager podrá recopilar pruebas de ese origen de datos.

Le recomendamos que se comunique con el destinatario para informarle si es necesario crear alguna regla personalizada AWS Config en su instancia de AWS Config.

He actualizado una regla personalizada que se usa en un marco compartido. ¿Tengo que tomar alguna medida?

Para actualizaciones de reglas en su entorno AWS

Al actualizar una regla personalizada en su entorno AWS, no es necesario realizar ninguna acción en Audit Manager. Audit Manager detecta y gestiona las actualizaciones de reglas de la forma que se describe en la siguiente tabla. Audit Manager no le notifica cuando se detecta una actualización de reglas.

Escenario	¿Qué hace Audit Manager?	Qué necesita
Se actualiza una regla personalizada en su instancia de AWS Config.	Audit Manager sigue informando de las conclusiones de esa regla mediante la definición de regla actualizada.	No es necesario ninguna acción.
Se elimina una regla personalizada en su instancia de AWS Config.	Audit Manager deja de informar de los resultados de la regla eliminada.	No es necesario ninguna acción. Si lo desea, puede editar los controles personalizados que utilizaban la regla eliminada como asignación de origen de datos. A continuación, puede eliminar la regla eliminada para limpiar la configuración de la origen de datos del control. De lo contrario, el nombre de la regla eliminada permanece como una asignación de origen de datos no utilizada.

Para actualizaciones de reglas fuera de su entorno AWS

En el entorno del destinatario AWS, Audit Manager no detecta la actualización de la regla. Esto se debe a que los remitentes y los destinatarios trabajan en entornos separados AWS. En la tabla siguiente se indican las acciones recomendadas para este escenario.

Su función	Escenario	Acción recomendada
Sender	• Compartió un marco que utiliza reglas personalizadas como asignación de origen de datos.	Póngase en contacto con el destinatario para informarle de la actualización. De esta forma, pueden realizar la misma

Su función	Escenario	Acción recomendada
	• Tras compartir el marco, actualizó o eliminó una de esas reglas en AWS Config.	actualización y mantenerse sincronizados con la definición de regla más reciente.
Recipie	• Ha aceptado un marco compartido que utiliza reglas personalizadas como asignación de origen de datos. • Tras volver a crear las reglas personalizadas en su instancia de AWS Config, el remitente actualizó o eliminó una de esas reglas.	Actualice la regla correspondiente en su propia instancia de AWS Config.

Solución de problemas de notificación

Puede utilizar la información de esta página para resolver problemas de notificación comunes en Audit Manager.

Temas

- He especificado un tema de Amazon SNS en Audit Manager, pero no recibo ninguna notificación
- He especificado un tema de FIFO, pero no recibo las notificaciones en el orden esperado

He especificado un tema de Amazon SNS en Audit Manager, pero no recibo ninguna notificación

Si su tema de Amazon SNS utiliza AWS KMS para el cifrado del servidor (SSE), es posible que le falten los permisos necesarios para su política de claves de AWS KMS. También es posible que no reciba las notificaciones si no ha suscrito un punto de conexión a su tema.

Si no recibe notificaciones, asegúrese de haber hecho lo siguiente:

- Adjuntó la política de permisos requerida a su clave de KMS. Hay un ejemplo de política disponible en la página de notificaciones de esta guía.

- Has suscrito un punto de conexión al tema a través del cual se envían las notificaciones. Cuando suscriba un punto de enlace de correo electrónico a un tema, recibirá un correo electrónico que le pedirá que confirme su suscripción. Debe confirmar la suscripción para comenzar a recibir notificaciones de correo electrónico. Para obtener más información, consulte Introducción en la Guía para desarrolladores de Amazon SNS.

He especificado un tema de FIFO, pero no recibo las notificaciones en el orden esperado

Audit Manager admite el envío de notificaciones a temas de FIFO SNS. Sin embargo, no se garantiza el orden en el que Audit Manager envía las notificaciones a sus temas de FIFO.

Solución de problemas de permisos y acceso

Puede utilizar la información de esta página para resolver problemas de permisos comunes en Audit Manager.

Temas

He seguido el procedimiento de configuración de Audit Manager, pero no tengo suficientes privilegios de IAM

El usuario, rol o grupo que usa para acceder a Audit Manager debe tener los permisos necesarios. Además, su política basada en la identidad no debería ser demasiado restrictiva. De lo contrario, la consola no funcionará según lo previsto. El procedimiento de configuración de esta guía proporciona una política que concede los permisos mínimos necesarios para configurar Audit Manager. Dependiendo de su caso de uso, es posible que necesite permisos más amplios y menos restrictivos.

Por ejemplo, recomendamos que los propietarios de las auditorías tengan acceso de administrador. Esto es para que puedan modificar la configuración de Audit Manager y gestionar recursos como las evaluaciones, los marcos, los controles y los informes de evaluación. Es posible que otros usuarios, como los delegados, solo necesiten acceso de gestión o acceso de solo lectura.

Asegúrese de añadir los permisos adecuados para su usuario, función o grupo. Para los propietarios de auditorías, la política recomendada es AWSAuditManagerAdministratorAccess. Para los delegados, puede utilizar este ejemplo que se proporciona en la página de ejemplos de políticas de IAM. Puede utilizar estas políticas de ejemplo como punto de partida y realizar los cambios que necesite para que se ajusten a sus necesidades.

Le recomendamos que dedique un tiempo a personalizar sus permisos para que se ajusten a sus requisitos específicos. Si necesita ayuda con los permisos de IAM, póngase en contacto con su administrador o con AWSSoporte.

He especificado a alguien como propietario de la auditoría, pero aún no tiene acceso completo a la evaluación. ¿Por qué sucede esto?

Especificar a alguien como propietario de una auditoría por sí solo no le proporciona acceso completo a una evaluación. Los propietarios de la auditoría también deben tener los permisos de IAM necesarios para acceder a los recursos de Audit Manager y gestionarlos. Es decir, además de especificar un usuario como propietario de la auditoría, también debe adjuntar a ese usuario las políticas de IAM necesarias. La razón es porque, al requerir ambas, Audit Manager garantiza que usted tiene el control total sobre todos los detalles de cada evaluación.

> **Note**
>
> Para los propietarios de auditorías, le recomendamos que utilice la política de AWSAuditManagerAdministratorAccess. Para obtener más información, consulte las Políticas recomendadas para personas de usuario en Audit Manager.

No puedo realizar una acción en Audit Manager

Si no tiene los permisos necesarios para usar la consola AWS Audit Manager o las operaciones de la API de Audit Manager, es probable que se produzca un error `AccessDeniedException`.

Para resolver este problema, debe ponerse en contacto con el administrador para recibir ayuda. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos en Audit Manager

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 obtener más información, consulte lo siguiente:

- Para obtener información acerca de si Audit Manager admite estas características, consulte ¿Cómo AWS Audit Manager funciona con IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte Proporcionar acceso a un usuario de IAM a otra Cuenta de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos a Cuentas de AWS de terceros, consulte Proporcionar acceso a Cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una identidad federada, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) 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.

Véase también

Las siguientes páginas contienen instrucciones para solucionar otros problemas que pueden deberse a la falta de permisos:

- No veo ningún control o conjunto de controles en mi evaluación
- La opción de regla personalizada no está disponible cuando configuro un origen de datos de control
- Cuando intento generar un informe de evaluación, aparece un error de acceso denegado

- Aparece un error de acceso denegado cuando intento generar un informe de evaluación con mi cuenta de administrador delegado
- No puedo habilitar el buscador de evidencias
- No puedo desactivar el buscador de evidencias
- Mi consulta de búsqueda falla en el buscador de evidencias
- He especificado un tema de Amazon SNS en Audit Manager, pero no recibo ninguna notificación

Cuotas y limitaciones para AWS Audit Manager

Su Cuenta de AWS tiene cuotas predeterminadas, anteriormente conocidas como límites, para cada servicio de Servicio de AWS. A menos que se indique otra cosa, cada cuota es específica de la región. Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

La mayoría de las cuotas de Audit Manager, aunque no todas, se enumeran en el espacio de nombres de AWS Audit Manager en la consola de Service Quotas. Para aprender cómo solicitar un aumento de cuota, consulte Administrar las cuotas de Audit Manager.

Cuotas de Audit Manager

Las cuotas de AWS Audit Manager que se incluyen a continuación se aplican a cada cuenta de Cuenta de AWS y a cada región.

Evaluaciones

- Número de evaluaciones activas por cuenta: 100

Informes de evaluación

- Número de elementos de prueba que puede añadir a un informe de evaluación:
  - Para los informes de la misma región (en los que la evaluación y el bucket S3 de destino del informe de evaluación se encuentran en el mismo lugarRegión de AWS): 22 000
  - Para los informes de distintas regiones (en los que la evaluación y el bucket S3 de destino del informe de evaluación se encuentran en el mismo lugarRegiones de AWS): 3500
  - En el caso de los informes en los que la evaluación correspondiente utiliza una información gestionada AWS KMS key por el cliente: 3500

Controles

- Número de tareas simultáneas por cuenta: 500

Prueba

- Tamaño máximo de un único archivo de pruebas manuales: 100 MB

- Número de cargas manuales diarias de pruebas por control: 100

> **Tip**
>
> Si necesita cargar una gran cantidad de pruebas manuales en un solo control, le recomendamos que cargue las pruebas en lotes durante varios días.

Marcos

- Número de marcos personalizados por cuenta: 100

> **Note**
>
> Las cuotas de marcos se aplican a todos los marcos personalizados compartidos de su biblioteca de marcos, independientemente de quién haya creado el marco.

Destinatarios de marcos personalizados compartidos

- Número de cuentas receptoras activas: 100

Acceso a API

- Número de transacciones por segundo (TPS) en todas las API: 20 TPS

Administrar las cuotas de Audit Manager

AWS Audit Manager se ha integrado con Service Quotas, un Servicio de AWS que le permite ver y administrar sus cuotas desde una ubicación central. Para obtener más información, consulte ¿Qué son las cuotas de servicio? en la Guía del usuario de Service Quotas. Con Service Quotas, resulta más sencillo buscar el valor de las cuotas de servicio de Audit Manager.

Para ver las service quotas de Audit Manager mediante la consola

1. Abra la consola de Service Quotas en https://console.aws.amazon.com/servicequotas/.
2. En el panel de navegación, elija Servicios de AWS.
3. En la lista Servicios de AWS services, busque y seleccioneAWS Audit Manager.

4. En la lista Service Quotas, puede ver el nombre de la Service quota, el valor aplicado (si está disponible), la cuota predeterminada de AWS y si el valor de cuota es ajustable.
5. Para ver información adicional sobre una cuota de servicio, como, por ejemplo, la descripción, elija el nombre de cuota.
6. (Opcional) Para solicitar un aumento de cuota, seleccione la cuota que desea aumentar, seleccione Solicitar aumento de cuota, escriba o seleccione la información necesaria y seleccione Solicitar.

Para obtener más información, consulte Solicitud de un aumento de cuota en la Guía del usuario de Service Quotas.

Seguridad en AWS Audit Manager

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 AWS nube. 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 cumplimiento aplicables AWS Audit Manager, consulte AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad yAWS 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 ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Audit Manager. En los siguientes temas, se le mostrará cómo configurar Audit Manager 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 Audit Manager.

Temas

Protección de datos en AWS Audit Manager

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS Audit Manager. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta 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 deAWS .

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 Audit Manager u otro Servicios de AWS mediante la consola, la API o AWS los SDK. AWS CLICualquier 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 información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Además de la recomendación anterior, recomendamos específicamente que los clientes de Audit Manager no incluyan información de identificación confidencial en los campos de formato libre al crear evaluaciones, controles personalizados, marcos personalizados y comentarios de las delegaciones.

Eliminación de datos de Audit Manager

Hay varias formas de eliminar los datos de Audit Manager.

Eliminación de datos al deshabilitar Audit Manager

Al deshabilitar Audit Manager, puede decidir si desea eliminar todos los datos de Audit Manager. Si decide eliminar sus datos, se eliminarán en un plazo de 7 días a partir de la desactivación de Audit Manager. Una vez eliminados los datos, no los puede recuperar.

Eliminación automática de datos

Algunos datos de Audit Manager se eliminan automáticamente después de un período de tiempo específico. Audit Manager conserva los datos de los clientes de la siguiente manera.

Tipo de datos	Periodo de retención de datos	Notas
Evidencia	Los datos se conservan durante 2 años desde el momento de la creación	Incluye evidencias automatizadas y evidencias manuales
Recursos creados por los clientes	Los datos se conservan indefinidamente	Incluye evaluaciones, informes de evaluación, controles personalizados y marcos personalizados

Eliminación manual de datos

Puede eliminar recursos de Audit Manager individuales en cualquier momento. Para obtener instrucciones, consulte lo siguiente:

- Eliminación de una evaluación
  - Consulte también: DeleteAssessmenten la referencia de la AWS Audit Manager API
- Eliminar un marco personalizado
  - Consulte también: DeleteAssessmentFrameworken la referencia de laAWS Audit Manager API
- Eliminar una solicitud de uso compartido
  - Consulte también: DeleteAssessmentFrameworkShareen la referencia de laAWS Audit Manager API
- Eliminación de una ejecución de evaluación
  - Consulte también: DeleteAssessmentReporten la referencia de laAWS Audit Manager API
- Eliminar un control personalizado
  - Consulte también: DeleteControlen la referencia de laAWS Audit Manager API

Para eliminar otros datos de recursos que pueda haber creado al utilizar Audit Manager, consulte lo siguiente:

- Eliminar un almacén de datos de eventos en la Guía del usuario deAWS CloudTrail
- Eliminar un bucket en la Guía del usuario de Amazon Simple Storage Service (Amazon S3).

Cifrado en reposo

Para cifrar los datos en reposo, Audit Manager utiliza el cifrado del lado del servidor Claves administradas por AWS para todos sus registros y almacenes de datos.

Sus datos se cifran mediante una clave gestionada por el cliente o una Clave propiedad de AWS, según la configuración que haya seleccionado. Si no proporciona una clave gestionada por el cliente, Audit Manager utilizará una Clave propiedad de AWS para cifrar el contenido. Todos los metadatos de los servicios en DynamoDB y Amazon S3 en Audit Manager se cifran mediante una Clave propiedad de AWS.

Audit Manager cifra los datos de la siguiente manera:

- Los metadatos del servicio almacenados en Amazon S3 se cifran Clave propiedad de AWS mediante un SSE-KMS.

- Los metadatos del servicio almacenados en DynamoDB se cifran en el servidor mediante KMS y una Clave propiedad de AWS.
- El contenido almacenado en DynamoDB se cifra en el lado del cliente mediante una clave administrada por el cliente o una Clave propiedad de AWS. La clave KMS se basa en la configuración que haya elegido.
- El contenido almacenado en Amazon S3 en Audit Manager se cifra mediante SSE-KMS. La clave KMS se basa en su selección y puede ser una clave administrada por el cliente o una Clave propiedad de AWS.
- Los informes de evaluación publicados en su bucket de S3 se cifran de la siguiente manera:
  - Si ha proporcionado una clave administrada por el cliente, sus datos se cifran mediante SSE-KMS.
  - Si utilizó el Clave propiedad de AWS, sus datos se cifran mediante el SSE-S3.

Cifrado en tránsito

Audit Manager proporciona puntos de enlace seguros y privados para cifrar datos en tránsito. Los puntos finales seguros y privados permiten AWS proteger la integridad de las solicitudes de API a Audit Manager.

Tránsito entre servicios

De forma predeterminada, todas las comunicaciones entre servicios se protegen mediante el cifrado de seguridad de la capa de transporte (TLS).

Administración de claves

Audit Manager admite Claves propiedad de AWS tanto claves administradas por el cliente como para cifrar todos los recursos de Audit Manager (evaluaciones, controles, marcos, pruebas e informes de evaluación guardados en depósitos de S3 en sus cuentas).

Recomendamos utilizar una clave administrada por el cliente. De este modo, puede ver y administrar las claves de cifrado que protegen sus datos, incluida la visualización de los registros de su uso en AWS CloudTrail. Al elegir una clave administrada por el cliente, Audit Manager crea una concesión en la clave de KMS para que pueda usarse para cifrar su contenido.

> **Warning**
>
> Después de eliminar o desactivar una clave KMS que se utiliza para cifrar recursos del Audit Manager, ya no podrá descifrar el recurso que estaba cifrado bajo esa clave KMS, lo que significa que los datos se vuelven irrecuperables.
> Eliminar una clave de KMS en AWS Key Management Service (AWS KMS) es destructivo y potencialmente peligroso. Para obtener más información sobre la eliminación de claves de KMS, consulte Eliminar AWS KMS keys en la Guía del usuario deAWS Key Management Service .

Puede especificar la configuración de cifrado al habilitar Audit Manager mediante la AWS Management ConsoleAPI Audit Manager o AWS Command Line Interface (AWS CLI). Para ver instrucciones, consulte Habilitar AWS Audit Manager.

Puede revisar y cambiar la configuración de cifrado en cualquier momento. Para ver instrucciones, consulte Cifrado de datos.

Para obtener más información sobre cómo configurar las claves administradas por el cliente, consulte Creación de claves en la Guía del usuario deAWS Key Management Service .

Administración de identidad y acceso para AWS Audit Manager

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Audit Manager. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

- AWS políticas gestionadas para AWS Audit Manager
- Solución de problemas de AWS Audit Manager identidad y acceso
- Uso de funciones vinculadas a servicios para AWS Audit Manager

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realice en Audit Manager.

Usuario de servicio: si utiliza el servicio de Audit Manager para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Audit Manager para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a alguna característica de la administración de costos de Audit Manager, consulte Solución de problemas de AWS Audit Manager identidad y acceso.

Administrador de servicio: si está a cargo de los recursos de Audit Manager en su empresa, probablemente tenga acceso completo a Audit Manager. Su trabajo consiste en determinar a qué características y recursos de Audit Manager deben acceder los 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 su empresa puede utilizar IAM con Audit Manager, consulte ¿Cómo AWS Audit Manager funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a Audit Manager. Para consultar ejemplos de políticas de Audit Manager basadas en identidades que puede utilizar en IAM, consulte Ejemplos de políticas basadas en la identidad para AWS Audit Manager.

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o

Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su 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 AWSen su Guía delAWS 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 deAWS 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 deAWS 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 deAWS 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 AWSy 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 AWSEl 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 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.

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 AWSempresa. 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 WAFPara 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 AWSPara más información sobre Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario deAWS 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 AWS Audit Manager funciona con IAM

Antes de utilizar IAM para administrar el acceso a Audit Manager, conozca qué características de IAM se pueden utilizar con Audit Manager.

Funciones de IAM que puede utilizar con AWS Audit Manager

Característica de IAM	Compatibilidad Audit Manager
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de políticas	Parcial
ACL	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo AWS Audit Manager funcionan otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para AWS Audit Manager

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.

AWS Audit Manager crea una política gestionada con el nombre `AWSAuditManagerAdministratorAccess` de los administradores de Audit Manager. Esta política otorga acceso administrativo completo a Audit Manager. Los administradores pueden adjuntar esta política a cualquier rol o usuario existente o crear un nuevo rol con esta política.

Políticas recomendadas para los usuarios de AWS Audit Manager

AWS Audit Manager le permite mantener la separación de funciones entre los diferentes usuarios y para las diferentes auditorías mediante el uso de diferentes políticas de IAM. Las dos personas de Audit Manager y sus políticas recomendadas se definen de la siguiente manera.

Persona	Descripción y política recomendada
Propietario de la auditoría	• Esta persona debe tener los permisos necesarios para gestionar las evaluaciones. AWS Audit Manager • La política que se recomienda usar para esta persona es la política administrada denominada AWSAuditManagerAdministratorAccess. Puede utilizar esta política como punto de partida y reducir estos permisos según sea necesario para que se ajusten a sus requisitos.

Persona	Descripción y política recomendada
Delegado	• Esta persona puede acceder a los conjuntos de control delegados de una evaluación. Puede actualizar el estado del control, añadir comentarios, enviar un conjunto de controles para su revisión y añadir evidencias al informe de evaluació n. • La política recomendada para esta persona es la siguiente política de ejemplo: Permitir a los usuarios acceso de administrador total a AWS Audit Manager. Puede utilizar esta política como punto de partida y realizar los cambios necesarios para adaptarlos a sus requisitos.

Ejemplos de políticas basadas en la identidad para AWS Audit Manager

Para ver ejemplos de políticas basadas en la identidad de Audit Manager, consulte Ejemplos de políticas basadas en la identidad para AWS Audit Manager.

Políticas basadas en recursos dentro AWS Audit Manager

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de políticas 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

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 políticas para AWS Audit Manager

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 AWS Audit Manager acciones, consulte Acciones definidas por AWS Audit Manager en la Referencia de autorización de servicios.

Las acciones políticas AWS Audit Manager utilizan el siguiente prefijo antes de la acción.

```
auditmanager
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "auditmanager:GetEvidenceDetails",
      "auditmanager:GetEvidenceEventDetails"
         ]
```

Puede utilizar caracteres comodín (*) para especificar varias acciones. Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Get`, incluya la siguiente acción.

```
"Action": "auditmanager:Get*"
```

Para ver ejemplos de políticas basadas en la identidad de Audit Manager, consulte Ejemplos de políticas basadas en la identidad para AWS Audit Manager.

Recursos políticos para AWS Audit Manager

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 los tipos de AWS Audit Manager recursos y sus ARN, consulte Recursos definidos por AWS Audit Manager en la Referencia de autorización de servicios. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recursos, consulte Acciones definidas por AWS Audit Manager.

Una evaluación de Audit Manager tiene el siguiente formato de Nombre de recurso de Amazon (ARN):

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

Un conjunto de controles de Audit Manager tiene el siguiente formato de ARN:

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/
${assessmentId}controlSet/${controlSetId}
```

Un control de Audit Manager tiene el siguiente formato de ARN:

```
arn:${Partition}:auditmanager:${Region}:${Account}:control/${controlId}
```

Para obtener más información acerca del formato de los ARN, consulte Nombres de recursos de Amazon (ARN).

Por ejemplo, para especificar la evaluación `i-1234567890abcdef0` en la instrucción, utilice el siguiente ARN.

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/
i-1234567890abcdef0"
```

Para especificar todas las instancias que pertenecen a una cuenta específica, utilice el carácter comodín (*).

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/*"
```

Algunas acciones de Audit Manager, como las empleadas para la creación de recursos, no se pueden llevar a cabo en un recurso específico. En dichos casos, debe utilizar el carácter comodín (*).

```
"Resource": "*"
```

En muchas acciones de la API de Audit Manager se utilizan varios recursos. Por ejemplo, `ListAssessments` devuelve una lista de metadatos de evaluación a los que pueden acceder las personas que hayan iniciado sesión Cuenta de AWSactualmente. Por lo tanto, un usuario debe tener permisos para ver las evaluaciones. Para especificar varios recursos en una única instrucción, separe los ARN con comas.

```
"Resource": [
      "resource1",
      "resource2"
```

Para ver una lista de tipos de recursos de Audit Manager y sus ARN, consulte Recursos definidos por AWS Audit Manager en la Guía del usuario de IAM. Para obtener información sobre las acciones

con las que puede especificar el ARN de cada recursos, consulte Acciones definidas por AWS Audit Manager.

Algunas acciones de la API de Audit Manager admiten varios recursos. Por ejemplo, `GetChangeLogs` accede a un `assessmentID`, `controlID` y `controlSetId`, por lo tanto, una entidad principal debe tener permisos para acceder a cada uno de estos recursos. Para especificar varios recursos en una única instrucción, separe los ARN con comas.

```
"Resource": [
      "assessmentId",
      "controlId",
      "controlSetId"
```

Claves de condición de la política para AWS Audit Manager

Admite claves de condición de políticas específicas del servicio	Parcial

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.

Cuando la entidad principal de una declaración de política es una entidad principal del servicio deAWS, recomendamos encarecidamente que utilice las claves de condición globales `aws:SourceArn` o `aws:SourceAccount` en la política. Puede utilizar estas claves de contexto de condición global para evitar que se produzca una situación de subdirección confusa. Las siguientes políticas documentadas muestran cómo se pueden utilizar las claves contextuales de condición

global `aws:SourceArn` y `aws:SourceAccount` en Audit Manager para evitar el problema del adjunto confundido.

- Ejemplo de política para un tema de SNS que se utiliza para las notificaciones de Audit Manager
- Ejemplo de política para una clave de KMS que se usa con un tema de SNS

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder a un usuario permiso para acceder a un recurso solo si está etiquetado con su nombre de usuario. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

Audit Manager no proporciona ninguna clave de condición específica del servicio, pero sí admite el uso de algunas claves de condición globales. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condiciónAWS globales en la Guía del usuario de IAM.

Listas de control de acceso (ACL) en AWS Audit Manager

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.

Control de acceso basado en atributos (ABAC) con AWS Audit Manager

Admite ABAC (etiquetas en las políticas)	Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿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.

Para obtener más información sobre el etiquetado de AWS Audit Manager recursos, consulte. Etiquetado de recursos de AWS Audit Manager

Uso de credenciales temporales con AWS Audit Manager

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 sobrel 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.

Sesiones de acceso directo para AWS Audit Manager

Admite Forward access sessions (FAS)	Sí

Cuando utiliza un usuario o un rol de IAM para realizar acciones en AWSél, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWSLas 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 detallada sobre las políticas a la hora de realizar solicitudes de FAS, consulte Forward access sessions.

Roles de servicio para AWS Audit Manager

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 AWS Audit Manager . Edite los roles de servicio solo cuando Audit Manager proporcione orientación para hacerlo.

Funciones vinculadas al servicio para AWS Audit Manager

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 AWSEl 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 sobre las funciones vinculadas al servicio, consulte. AWS Audit ManagerUso de funciones vinculadas a servicios para AWS Audit Manager

Ejemplos de políticas basadas en la identidad para AWS Audit Manager

De forma predeterminada, los usuarios y roles no tienen permiso para crear o modificar recursos del Audit Manager. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. 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.

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 AWS Audit Manager, incluido el formato de los ARN para cada tipo de recurso, consulte Acciones, recursos y claves de condición para AWS Audit Manager en la Referencia de autorizaciones de servicio.

Temas

- Prácticas recomendadas sobre las políticas
- Permita los permisos mínimos necesarios para activar Audit Manager
- Permitir a los usuarios acceso de administrador total a AWS Audit Manager
- Permita que la administración de los usuarios acceda a AWS Audit Manager
- Permita a los usuarios el acceso de solo lectura a AWS Audit Manager
- Cómo permitir a los usuarios consultar sus propios permisos
- Permitir AWS Audit Manager enviar notificaciones a temas de Amazon SNS
- Permita a los usuarios realizar consultas de búsqueda en el buscador de evidencias

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Audit Manager 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 políticasAWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWSLe 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 porAWS o las políticas administradas porAWS 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 más información, consulte Elementos de política 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 AWSsu 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.

Permita los permisos mínimos necesarios para activar Audit Manager

En este ejemplo se muestra cómo puede permitir que se habiliten cuentas sin función de administrador para habilitar AWS Audit Manager.

> **Note**
>
> Lo que ofrecemos aquí es una política básica que concede los permisos mínimos necesarios para activar Audit Manager. Todos los permisos de la política siguiente son obligatorios. Si omite alguna parte de esta política, no podrá habilitar Audit Manager.
> Le recomendamos que dedique un tiempo a personalizar sus permisos para que se adapten a sus necesidades específicas. Si necesita ayuda, póngase en contacto con su administrador o con AWS Support.

Para conceder el acceso mínimo necesario para activar Audit Manager, utilice los siguientes permisos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "auditmanager:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "CreateEventsAccess",
```

```
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Effect": "Allow",
            "Action": "kms:ListAliases",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        }
    ]
}
```

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 intenta realizar.

Permitir a los usuarios acceso de administrador total a AWS Audit Manager

Los siguientes ejemplos de políticas otorgan acceso de administrador total a AWS Audit Manager.

- Ejemplo 1 (política gestionada, `AWSAuditManagerAdministratorAccess`)
- Ejemplo 2 (permisos de destino del informe de evaluación)
- Ejemplo 3 (permisos de destino de exportación)
- Ejemplo 4 (Permisos para activar el buscador de evidencias)
- Ejemplo 5 (Permisos para desactivar el buscador de evidencias)

Ejemplo 1 (política gestionada, **`AWSAuditManagerAdministratorAccess`**)

La política en este ejemplo es la política administrada, `AWSAuditManagerAdministratorAccess`. Esta política incluye la capacidad de activar y desactivar Audit Manager, la posibilidad de cambiar la configuración de Audit Manager y la capacidad de gestionar todos los recursos del Audit Manager, como las evaluaciones, los marcos, los controles y los informes de evaluación.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
```

```
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
```

```
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Ejemplo 2 (permisos de destino del informe de evaluación)

Esta política le concede permiso para acceder a un bucket de S3 específico y para añadir y eliminar archivos de él. Esto le permite utilizar el bucket especificado como destino del informe de evaluación en Audit Manager.

Sustituya el *texto del marcador* de posición por su propia información. Incluya el bucket de S3 que utiliza como destino del informe de evaluación y la clave KMS que utiliza para cifrar los informes de evaluación.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "s3:PutObject",
               "s3:GetObject",
               "s3:ListBucket",
               "s3:DeleteObject",
               "s3:GetBucketLocation",
               "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
        }
    ]
},
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
```

```
}
```

Ejemplo 3 (permisos de destino de exportación)

La siguiente política permite CloudTrail enviar los resultados de las consultas del buscador de evidencias al bucket S3 especificado. Como práctica recomendada de seguridad, la clave de condición global de IAM `aws:SourceArn` ayuda a garantizar que solo se CloudTrail escriba en el depósito de S3 para el almacén de datos de eventos.

Sustituya el *`texto del marcador`* de posición por su propia información, de la siguiente manera:

- Reemplace *`DOC-EXAMPLE-DESTINATION-BUCKET`* con el bucket de S3 que utiliza como destino de exportación.
- Sustituya *`myQueryRunningla región`* Región de AWS por la que corresponda a su configuración.
- Sustituya *`myAccountID por`* el Cuenta de AWS ID que se utiliza para. CloudTrail Puede que no coincida con el ID Cuenta de AWS del bucket de S3. Si se trata de un almacén de datos de eventos de la organización, debes usarlo Cuenta de AWS para la cuenta de administración.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
```

```
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

Ejemplo 4 (Permisos para activar el buscador de evidencias)

Se requiere la siguiente política de permisos si desea activar y utilizar la característica de búsqueda de evidencias. Esta declaración de política permite a Audit Manager crear un banco de datos de eventos de CloudTrail Lake y ejecutar consultas de búsqueda.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
           "Sid": "ManageCloudTrailLakeQueryAccess",
           "Effect": "Allow",
           "Action": [
               "cloudtrail:StartQuery",
               "cloudtrail:DescribeQuery",
               "cloudtrail:GetQueryResults",
               "cloudtrail:CancelQuery"
           ],
           "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
        },
        {
           "Sid": "ManageCloudTrailLakeAccess",
           "Effect": "Allow",
           "Action": [
                "cloudtrail:CreateEventDataStore"
           ],
           "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
         }
    ]
}
```

Ejemplo 5 (Permisos para desactivar el buscador de evidencias)

Este ejemplo de política otorga permiso para deshabilitar la característica de búsqueda de evidencias en Audit Manager. Esto implica eliminar el almacén de datos de eventos que se creó cuando habilitó la característica por primera vez.

Antes de utilizar esta política, sustituya el *texto del marcador* por su propia información. Debe especificar el UUID del almacén de datos de eventos que se creó al activar el buscador de evidencias. Puede recuperar el ARN del almacén de datos de eventos desde la configuración de Audit Manager. Para obtener más información, consulte GetSettings en la Referencia de la API deAWS Audit Manager .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "cloudtrail:DeleteEventDataStore",
               "cloudtrail:UpdateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:::event-data-store-UUID"
        }
    ]
}
```

Permita que la administración de los usuarios acceda a AWS Audit Manager

En este ejemplo se muestra cómo puede permitir el acceso de administración de no administradores a AWS Audit Manager.

Esta política permite gestionar todos los recursos de Audit Manager (evaluaciones, marcos y controles), pero no permite activar o desactivar Audit Manager ni modificar la configuración del Audit Manager.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:GetAccountStatus",
                "auditmanager:ListAssessmentFrameworks",
                "auditmanager:CreateAssessmentFramework",
                "auditmanager:GetAssessmentFramework",
                "auditmanager:UpdateAssessmentFramework",
                "auditmanager:DeleteAssessmentFramework",
                "auditmanager:ListAssessmentReports",
                "auditmanager:ListAssessments",
                "auditmanager:CreateAssessment",
                "auditmanager:ListControls",
                "auditmanager:CreateControl",
                "auditmanager:GetControl",
```

```
                "auditmanager:UpdateControl",
                "auditmanager:DeleteControl",
                "auditmanager:ListKeywordsForDataSource",
                "auditmanager:GetDelegations",
                "auditmanager:ValidateAssessmentReportIntegrity",
                "auditmanager:ListNotifications",
                "auditmanager:GetServicesInScope",
                "auditmanager:GetSettings",
                "auditmanager:ListTagsForResource",
                "auditmanager:TagResource",
                "auditmanager:UntagResource"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Permita a los usuarios el acceso de solo lectura a AWS Audit Manager

Esta política otorga acceso de solo lectura a AWS Audit Manager recursos como evaluaciones, marcos y controles.

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

```
                "auditmanager:Get*",
                "auditmanager:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

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 o. AWS CLI 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 AWS Audit Manager enviar notificaciones a temas de Amazon SNS

Las políticas de este ejemplo conceden a Audit Manager permisos para enviar notificaciones a un tema de Amazon SNS existente.

- Ejemplo 1: Si desea recibir notificaciones de Audit Manager, utilice este ejemplo para añadir permisos a la política de acceso a los temas de SNS.
- Ejemplo 2: Si su tema de SNS utiliza AWS Key Management Service (AWS KMS) para el cifrado del lado del servidor (SSE), utilice este ejemplo para añadir permisos a la política de acceso a claves de KMS.

En el siguiente ejemplo de política, la entidad principal que obtiene los permisos es la entidad principal del servicio Audit Manager, que es `auditmanager.amazonaws.com`. Cuando la entidad principal de una declaración de política es una entidad principal del servicio deAWS, recomendamos encarecidamente que utilice las claves de condición globales `aws:SourceArn` o `aws:SourceAccount` en la política. Puede utilizar estas claves de contexto de condición global para evitar que se produzca una situación de subdirección confusa.

Ejemplo 1 (Permisos para el tema SNS)

Esta declaración de política permite a Audit Manager publicar eventos en el tema SNS especificado. Cualquier solicitud de publicación sobre el tema de SNS especificado debe cumplir las condiciones de la política.

Antes de utilizar esta política, sustituya el *`texto del marcador`* por su propia información. Tome nota de lo siguiente:

- Si utiliza la clave de condición `aws:SourceArn` en esta política, el valor debe ser el ARN del recurso Audit Manager del que proviene la notificación. En el ejemplo siguiente, `aws:SourceArn` utiliza un comodín (`*`) como identificador del recurso. Esto permite todas las solicitudes que provienen de Audit Manager en todos los recursos de Audit Manager. Con la clave de condición global `aws:SourceArn`, puede utilizar el operador de condición `StringLike` o `ArnLike`. La práctica recomendada consiste en utilizar `ArnLike`.

- Si utiliza la clave de condición `aws:SourceAccount`, puede utilizar el operador de condición `StringEquals` o `StringLike`. La práctica recomendada consiste en usar `StringEquals` para implementar privilegios mínimos.
- Si utiliza ambos `aws:SourceAccount` y `aws:SourceArn`, los valores de la cuenta deben mostrar el mismo ID de cuenta.

```
{
  "Version": "2012-10-17",
  "Statement": {
      "Sid": "AllowAuditManagerToUseSNSTopic",
      "Effect": "Allow",
      "Principal": {
        "Service": "auditmanager.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:accountID:topicName",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountID"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
    }
}
```

El siguiente ejemplo alternativo usa solo la clave de condición `aws:SourceArn`, con el operador de condición `StringLike`:

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
```

El siguiente ejemplo alternativo usa solo la clave de condición `aws:SourceAccount`, con el operador de condición `StringLike`:

```
    "Condition": {
```

```
      "StringLike": {
        "aws:SourceAccount": "accountID"
       }
     }
```

Ejemplo 2 (permisos para la clave de KMS que se adjunta al tema de SNS)

Esta declaración de política permite a Audit Manager utilizar la clave KMS para generar la clave de datos que utiliza para cifrar un tema SNS. Cualquier solicitud de uso de la clave KMS para la operación especificada debe cumplir las condiciones de la política.

Antes de utilizar esta política, sustituya el *texto del marcador* por su propia información. Tome nota de lo siguiente:

- Si usa la clave de condición `aws:SourceArn` en esta política, el valor debe ser el ARN del recurso que se está cifrando. Por ejemplo, en este caso, es el tema del SNS de su cuenta. Establezca el valor en el ARN o un patrón ARN con caracteres comodín (*). Con la clave de condición `aws:SourceArn`, puede utilizar el operador de condición `StringLike` o `ArnLike`. La práctica recomendada consiste en utilizar `ArnLike`.
- Si utiliza la clave de condición `aws:SourceAccount`, puede utilizar el operador de condición `StringEquals` o `StringLike`. La práctica recomendada consiste en usar `StringEquals` para implementar privilegios mínimos. Puede usar `aws:SourceAccount` si no conoce el ARN del tema de SNS.
- Si utiliza ambos `aws:SourceAccount` y `aws:SourceArn`, los valores de la cuenta deben mostrar el mismo ID de cuenta.

```
{
     "Version": "2012-10-17",
     "Statement": {
       "Sid": "AllowAuditManagerToUseKMSKey",
       "Effect": "Allow",
       "Principal": {
           "Service": "auditmanager.amazonaws.com"
       },
       "Action": [
           "kms:Decrypt",
           "kms:GenerateDataKey"
       ],
       "Resource": "arn:aws:kms:region:accountID:key/*",
```

```
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "accountID"
             }
             "ArnLike": {
                  "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
             }
       }
     }
  ]
}
```

El siguiente ejemplo alternativo usa solo la clave de condición `aws:SourceArn`, con el operador de condición `StringLike`:

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
        }
      }
```

El siguiente ejemplo alternativo usa solo la clave de condición `aws:SourceAccount`, con el operador de condición `StringLike`:

```
   "Condition": {
     "StringLike": {
       "aws:SourceAccount": "accountID"
     }
    }
```

Permita a los usuarios realizar consultas de búsqueda en el buscador de evidencias

La siguiente política otorga permisos para realizar consultas en un banco de datos de eventos de CloudTrail Lake. Esta política de permisos es necesaria si desea utilizar la característica de búsqueda de pruebas.

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

```
            "Action": [
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "*"
        }
    ]
}
```

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio de llamadas puede ser manipulado para utilizar sus permisos para actuar sobre los recursos de otro cliente cuando no tiene permiso para hacerlo. Para evitarlo, Amazon Web Services proporciona herramientas que le ayudan a proteger sus datos en todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Recomendamos utilizar las claves de contexto de condición `aws:SourceAccount`global `aws:SourceArn`y las claves de contexto en las políticas de recursos para limitar los permisos que se AWS Audit Manager conceden a otro servicio para acceder a sus recursos.

- Utilice `aws:SourceArn` si desea que solo se asocie un recurso al acceso entre servicios. También puede utilizar `aws:SourceArn` con un comodín (`*`) si desea especificar varios recursos.

  Por ejemplo: puede utilizar un tema de Amazon SNS para recibir notificaciones de actividad de Audit Manager. En este caso, en la política de acceso al tema de SNS, el valor ARN de `aws:SourceArn` es el recurso Audit Manager del que proviene la notificación. Como es probable que tenga varios recursos de Audit Manager, le recomendamos que utilice `aws:SourceArn` con un comodín. Esto le permite especificar todos los recursos de Audit Manager en su política de acceso a los temas de SNS.
- Utilice `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

- Si el valor de `aws:SourceArn` no contiene el ID de cuenta, como un ARN de bucket de Amazon S3, debe utilizar ambas claves de contexto de condición global para limitar los permisos.
- Si utiliza las dos condiciones y el valor `aws:SourceArn` contiene el ID de la cuenta, el valor `aws:SourceAccount` y la cuenta del valor `aws:SourceArn` deben mostrar el mismo ID de cuenta cuando se empleen en la misma instrucción de política.
- La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el Nombre de recurso de Amazon (ARN) completo del recurso o si está especificando varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con caracteres comodines (*) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Audit Manager confundió al soporte adjunto

Audit Manager proporciona un soporte adjunto confuso en los siguientes escenarios. Estos ejemplos de políticas muestran cómo se pueden utilizar las claves de condición `aws:SourceArn` y `aws:SourceAccount` para evitar el problema del suplente confuso.

- Política de ejemplo: el tema de SNS que utiliza para recibir las notificaciones de Audit Manager
- Ejemplo de política: la clave de KMS que se utiliza para cifrar el tema de SNS

Audit Manager no proporciona un soporte adjunto confuso para la clave administrada por el cliente que usted proporciona en la configuración Cifrado de datos de Audit Manager. Si ha proporcionado su propia clave administrada por el cliente, no puede usar las condiciones `aws:SourceAccount` ni `aws:SourceArn` en esa política de claves de KMS.

AWS políticas gestionadas para AWS Audit Manager

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 porAWS en la Guía del usuario de IAM.

Temas

- AWS política gestionada: AWSAuditManagerAdministratorAccess
- AWS política gestionada: AWSAuditManagerServiceRolePolicy
- AWS Audit Manager actualizaciones de las políticas AWS gestionadas

AWS política gestionada: AWSAuditManagerAdministratorAccess

Puede adjuntar la política de `AWSAuditManagerAdministratorAccess` a las identidades de IAM.

Esta política otorga permisos administrativos que permiten el acceso total de la administración a AWS Audit Manager. Este acceso incluye la capacidad de habilitar y deshabilitar AWS Audit Manager, cambiar la configuración y administrar todos los recursos de Audit Manager AWS Audit Manager, como las evaluaciones, los marcos, los controles y los informes de evaluación.

AWS Audit Manager requiere amplios permisos en varios AWS servicios. Esto se debe a que AWS Audit Manager se integra con varios AWS servicios para recopilar pruebas automáticamente de Cuenta de AWS los servicios incluidos en el ámbito de una evaluación.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `Audit Manager`: Permite a las entidades principales tener plenos permisos sobre los recursos AWS Audit Manager .
- `Organizations`: Permite a las entidades principales enumerar las cuentas y las unidades organizativas y registrar o anular el registro de un administrador delegado. Esto es necesario para poder habilitar la compatibilidad con varias cuentas y poder AWS Audit Manager realizar evaluaciones en varias cuentas y consolidar las pruebas en una cuenta de administrador delegado.

- `iam`: Permite a las entidades principales obtener y enumerar los usuarios en IAM y crear un rol vinculado al servicio. Esto es necesario para poder designar a los responsables y delegados de la auditoría para una evaluación. Esta política también permite a las entidades principales eliminar el rol vinculado al servicio y recuperar el estado de eliminación. Esto es necesario para AWS Audit Manager poder limpiar los recursos y eliminar el rol vinculado al servicio si decide deshabilitar el servicio en el. AWS Management Console
- `s3`: Permite a las entidades principales enumerar los buckets de Amazon Simple Storage Service (Amazon S3) disponibles. Esta capacidad es necesaria para que pueda designar el bucket de S3 en el que desea almacenar los informes de evidencias o cargar las evidencias manualmente.
- `kms`: Permite a las entidades principales enumerar y describir claves, enumerar alias y crear concesiones. Esto es necesario para que pueda elegir las claves administradas por el cliente para el cifrado de datos.
- `sns`: Permite a las entidades principales publicar temas de suscripción en Amazon SNS. Esto es necesario para que pueda especificar a qué tema de SNS quiere que AWS Audit Manager envíe las notificaciones.
- `events`— Permite a los directores enumerar los cheques y gestionarlos desde. AWS Security HubEsto es necesario para AWS Audit Manager poder recopilar automáticamente AWS Security Hub los resultados de los AWS servicios que supervisan. AWS Security HubA continuación, puede convertir estos datos en evidencias para incluirlas en sus evaluaciones AWS Audit Manager .
- `tag`: Permite a las entidades principales recuperar los recursos etiquetados. Esto es necesario para poder utilizar las etiquetas como filtro de búsqueda al explorar los marcos, los controles y las evaluaciones AWS Audit Manager.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
```

```
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
```

```
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
```

```
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
```

```
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS política gestionada: AWSAuditManagerServiceRolePolicy

No puede asociar `AWSAuditManagerServiceRolePolicy` a sus entidades IAM. Esta política está asociada a un rol vinculado al servicio`AWSServiceRoleForAuditManager`, que permite AWS Audit Manager realizar acciones en su nombre. Para obtener más información, consulte Uso de roles vinculados a servicios para AWS Audit Manager.

La política de permisos de funciones, `AWSAuditManagerServiceRolePolicy`, permite que AWS Audit Manager recopile evidencias automatizadas haciendo lo siguiente en su nombre:

- Recopilar datos de las siguientes fuentes de datos:
  - Eventos de gestión desde AWS CloudTrail
  - Controles de cumplimiento desde Reglas de AWS Config
  - Controles de conformidad de AWS Security Hub
- Utilice las llamadas a la API para describir las configuraciones de sus recursos para los siguientes Servicios de AWS.

> **Tip**
>
> Para obtener más información sobre las llamadas a la API que Audit Manager utiliza para recopilar evidencias de estos servicios, consulte Se admiten llamadas a la API para orígenes de datos de control personalizadas en esta guía.

- AWS Certificate Manager
- AWS Backup
- Amazon Bedrock
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Logs
- Grupos de usuarios de Amazon Cognito
- AWS Config
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2
- Amazon Elastic Container Service
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache
- Elastic Load Balancing
- Amazon EMR
- Amazon EventBridge
- Amazon Data Firehose
- Amazon FSx
- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- Amazon Kinesis
- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Managed Streaming for Apache Kafka
- AWS Organizations
- Amazon Relational Database Service

- Amazon Redshift
- Amazon Route 53
- Amazon S3
- AWS Security Hub
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS WAF

Detalles de los permisos

`AWSAuditManagerServiceRolePolicy`permite AWS Audit Manager realizar las siguientes acciones en los recursos especificados:

- `acm:GetAccountConfiguration`
- `acm:ListCertificates`
- `backup:ListRecoveryPointsByResource`
- `bedrock:GetCustomModel`
- `bedrock:GetFoundationModel`
- `bedrock:GetModelCustomizationJob`
- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:ListCustomModels`
- `bedrock:ListFoundationModels`
- `bedrock:ListModelCustomizationJobs`
- `cloudtrail:DescribeTrails`
- `cloudtrail:LookupEvents`
- `cloudwatch:DescribeAlarms`
- `cloudwatch:DescribeAlarmsForMetric`
- `cloudwatch:GetMetricStatistics`
- `cloudwatch:ListMetrics`
- `cognito-idp:DescribeUserPool`
- `config:DescribeConfigRules`

- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeTable
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections

- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors

- iam:GenerateCredentialReport
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration

- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDbClusterEndpoints
- rds:DescribeDbClusterParameterGroups
- rds:DescribeDbClusters
- rds:DescribeDBInstances
- rds:DescribeDbSecurityGroups
- redshift:DescribeClusters
- route53:GetQueryLoggingConfig
- s3:GetBucketPolicy
  - Esta acción de la API opera dentro del ámbito de Cuenta de AWS donde service-linked-role esté disponible. No puede acceder a las políticas de bucket entre cuentas.
- s3:GetBucketPublicAccessBlock
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- securityhub:DescribeStandards
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:ListRuleGroups

- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:ListActivatedRulesInRuleGroup

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "acm:GetAccountConfiguration",
    "acm:ListCertificates",
    "backup:ListRecoveryPointsByResource",
    "bedrock:GetCustomModel",
    "bedrock:GetFoundationModel",
    "bedrock:GetModelCustomizationJob",
    "bedrock:GetModelInvocationLoggingConfiguration",
    "bedrock:ListCustomModels",
    "bedrock:ListFoundationModels",
    "bedrock:ListModelCustomizationJobs",
    "cloudtrail:DescribeTrails",
    "cloudtrail:LookupEvents",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:DescribeAlarmsForMetric",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cognito-idp:DescribeUserPool",
    "config:DescribeConfigRules",
    "config:DescribeDeliveryChannels",
    "config:ListDiscoveredResources",
    "directconnect:DescribeDirectConnectGateways",
    "directconnect:DescribeVirtualGateways",
    "dynamodb:DescribeTable",
    "dynamodb:ListBackups",
    "dynamodb:ListGlobalTables",
    "dynamodb:ListTables",
    "ec2:DescribeAddresses",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeFlowLogs",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
```

```
    "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
    "ec2:DescribeLocalGateways",
    "ec2:DescribeLocalGatewayVirtualInterfaces",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:GetEbsEncryptionByDefault",
    "ecs:DescribeClusters",
    "eks:DescribeAddonVersions",
    "elasticache:DescribeCacheClusters",
    "elasticache:DescribeServiceUpdates",
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeFileSystems",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeSslPolicies",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticmapreduce:ListClusters",
    "elasticmapreduce:ListSecurityConfigurations",
    "events:DescribeRule",
    "events:ListConnections",
    "events:ListEventBuses",
    "events:ListEventSources",
    "events:ListRules",
    "firehose:ListDeliveryStreams",
    "fsx:DescribeFileSystems",
    "guardduty:ListDetectors",
    "iam:GenerateCredentialReport",
    "iam:GetAccountAuthorizationDetails",
    "iam:GetAccountPasswordPolicy",
    "iam:GetAccountSummary",
    "iam:GetCredentialReport",
    "iam:ListEntitiesForPolicy",
    "iam:ListGroupPolicies",
    "iam:ListGroups",
```

```
    "iam:ListOpenIdConnectProviders",
    "iam:ListPolicies",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "iam:ListSamlProviders",
    "iam:ListUserPolicies",
    "iam:ListUsers",
    "iam:ListVirtualMFADevices",
    "kafka:ListClusters",
    "kafka:ListKafkaVersions",
    "kinesis:ListStreams",
    "kms:DescribeKey",
    "kms:GetKeyPolicy",
    "kms:GetKeyRotationStatus",
    "kms:ListGrants",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "lambda:ListFunctions",
    "license-manager:ListAssociationsForLicenseConfiguration",
    "license-manager:ListLicenseConfigurations",
    "license-manager:ListUsageForLicenseConfiguration",
    "logs:DescribeDestinations",
    "logs:DescribeExportTasks",
    "logs:DescribeLogGroups",
    "logs:DescribeMetricFilters",
    "logs:DescribeResourcePolicies",
    "logs:FilterLogEvents",
    "organizations:DescribeOrganization",
    "organizations:DescribePolicy",
    "rds:DescribeCertificates",
    "rds:DescribeDbClusterEndpoints",
    "rds:DescribeDbClusterParameterGroups",
    "rds:DescribeDbClusters",
    "rds:DescribeDBInstances",
    "rds:DescribeDbSecurityGroups",
    "redshift:DescribeClusters",
    "route53:GetQueryLoggingConfig",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketVersioning",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:ListAllMyBuckets",
    "securityhub:DescribeStandards",
    "sns:ListTopics",
```

```
    "sqs:ListQueues",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:ListRuleGroups",
    "waf-regional:ListSubscribedRuleGroups",
    "waf-regional:ListWebACLs",
    "waf:ListActivatedRulesInRuleGroup"
   ],
   "Resource": "*",
   "Sid": "AuditManagerAPICallAccess"
  },
  {
   "Sid": "AuditManagerS3GetBucketPolicyAccess",
   "Effect": "Allow",
   "Action": [
    "s3:GetBucketPolicy"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": [
      "${aws:PrincipalAccount}"
     ]
    }
   }
  },
  {
   "Sid": "CreateEventsAccess",
   "Effect": "Allow",
   "Action": [
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
   "Condition": {
    "StringEquals": {
     "events:detail-type": "Security Hub Findings - Imported"
    },
    "Null": {
     "events:source": "false"
    },
    "ForAllValues:StringEquals": {
     "events:source": [
      "aws.securityhub"
     ]
    }
```

```
    }
   },
   {
    "Sid": "EventsAccess",
    "Effect": "Allow",
    "Action": [
     "events:DeleteRule",
     "events:DescribeRule",
     "events:EnableRule",
     "events:DisableRule",
     "events:ListTargetsByRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
   }
  ]
}
```

AWS Audit Manager actualizaciones de las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas AWS Audit Manager desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del AWS Audit Manager documento.

Cambio	Descripción	Fecha
AWSAuditManagerServiceRolePolicy : actualización de una política actual	El rol vinculado al servicio ahora permite AWS Audit Manager realizar la `s3:GetBucketPolicy` acción. Esta acción de la API es necesaria para respaldar la v1 del marco de mejores prácticas de IA generativa deAWS. Le permite a Audit Manager recopilar pruebas automatizadas sobre las restricciones de políticas vigentes para los conjuntos de datos de entrenamiento de datos de modelos de IA generativa.	12/06/2023

Cambio	Descripción	Fecha
	La `GetBucketPolicy` acción opera dentro del ámbito en el que Cuenta de AWS service-linked-role esté disponible. No puede acceder a las políticas de bucket entre cuentas.	

Cambio	Descripción	Fecha
AWSAuditManagerServiceRolePolicy : actualización de una política actual	Hemos añadido los siguientes permisos a. `AWSAuditManagerServiceRolePolicy` AWS Audit Manager ahora puede realizar las siguientes acciones para recopilar pruebas automatizadas sobre los recursos de su propiedad Cuenta de AWS. • `acm:GetAccountConfiguration` • `acm:ListCertificates` • `backup:ListRecoveryPointsByResource` • `bedrock:GetCustomModel` • `bedrock:GetFoundationModel` • `bedrock:GetModelCustomizationJob` • `bedrock:GetModelInvocationLoggingConfiguration` • `bedrock:ListCustomModels` • `bedrock:ListFoundationModels` • `bedrock:ListModelCustomizationJobs` • `cloudtrail:LookupEvents` • `cloudwatch:DescribeAlarmsForMetric` • `cloudwatch:GetMetricStatistics` • `cloudwatch:ListMetrics` • `directconnect:DescribeDirectConnectGateways` • `directconnect:DescribeVirtualGateways` • `dynamodb:ListBackups`	11/06/2023

Cambio	Descripción	Fecha
	• dynamodb:ListGlobalTables • ec2:DescribeAddresses • ec2:DescribeCustomerGateways • ec2:DescribeEgressOnlyInternetGateways • ec2:DescribeInternetGateways • ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations • ec2:DescribeLocalGateways • ec2:DescribeLocalGatewayVirtualInterfaces • ec2:DescribeNatGateways • ec2:DescribeTransitGateways • ec2:DescribeVpcPeeringConnections • ec2:DescribeVpnConnections • ec2:DescribeVpnGateways • ec2:GetEbsDefaultKmsKeyId • ec2:GetEbsEncryptionByDefault • ecs:DescribeClusters • eks:DescribeAddonVersions • elasticache:DescribeCacheClusters • elasticache:DescribeServiceUpdates • elasticfilesystem:DescribeAccessPoints • elasticloadbalancing:DescribeLoadBalancers	

Cambio	Descripción	Fecha
	• elasticloadbalancing:DescribeSslPolicies • elasticloadbalancing:DescribeTargetGroups • elasticmapreduce:ListClusters • elasticmapreduce:ListSecurityConfigurations • events:ListConnections • events:ListEventBuses • events:ListEventSources • events:ListRules • firehose:ListDeliveryStreams • fsx:DescribeFileSystems • iam:GetAccountPasswordPolicy • iam:GetCredentialReport • iam:ListOpenIdConnectProviders • iam:ListSamlProviders • iam:ListVirtualMFADevices • kafka:ListClusters • kafka:ListKafkaVersions • kinesis:ListStreams • lambda:ListFunctions • logs:DescribeDestinations • logs:DescribeExportTasks • logs:DescribeLogGroups • logs:DescribeMetricFilters • logs:DescribeResourcePolicies • logs:FilterLogEvents • rds:DescribeCertificates	

Cambio	Descripción	Fecha
	• rds:DescribeDbClusterEndpoints • rds:DescribeDbClusterParameterGroups • rds:DescribeDbClusters • rds:DescribeDbSecurityGroups • redshift:DescribeClusters • s3:GetBucketPublicAccessBlock • s3:GetBucketVersioning • sns:ListTopics • sqs:ListQueues • waf-regional:GetLoggingConfiguration • waf-regional:ListRuleGroups • waf-regional:ListSubscribedRuleGroups • waf-regional:ListWebACLs	
AWSAuditManagerServiceRolePolicy : actualización de una política actual	Hemos agregado los siguientes permisos a AWSAuditManagerServiceRolePolicy : • dynamodb:DescribeTable • dynamodb:ListTables • ec2:DescribeVolumes • kms:GetKeyPolicy • kms:GetKeyRotationStatus • kms:ListKeyPolicies • rds:DescribeDBInstances • redshift:DescribeClusters • s3:GetEncryptionConfiguration • s3:ListAllMyBuckets	07/07/2022

Cambio	Descripción	Fecha
AWSAuditManagerServiceRolePolicy: actualización de una política actual	El rol vinculado al servicio ahora permite realizar AWS Audit Manager la acción. `organizations:DescribeOrganization` También hemos reducido el alcance del recurso `CreateEventsAccess` , pasando de ser un carácter comodín (*) a un tipo específico de recurso (`arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver`). Por último, añadimos un operador de condición `Null` a la clave de condición `events:source` para confirmar que existe un valor de origen y que su valor no es nulo.	20/05/2022
AWSAuditManagerAdministratorAccess: actualización de una política actual	Hemos actualizado la política de condiciones de clave `events:source` para que refleje que se trata de una clave con varios valores.	29/04/2022
AWSAuditManagerServiceRolePolicy: actualización de una política actual	Hemos actualizado la política de condiciones de clave `events:source` para que refleje que se trata de una clave con varios valores.	16/03/2022
AWS Audit Manager comenzó a rastrear los cambios	AWS Audit Manager comenzó a rastrear los cambios de sus políticas AWS gestionadas.	05/06/2021

Solución de problemas de AWS Audit Manager identidad y acceso

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Audit Manager e IAM.

Temas

- No estoy autorizado a realizar ninguna acción en AWS Audit Manager

- No estoy autorizado a realizar iam: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS Audit Manager recursos

No estoy autorizado a realizar ninguna acción en AWS Audit Manager

El `AccessDeniedException` error aparece cuando un usuario no tiene permiso para usar AWS Audit Manager las operaciones de la API Audit Manager.

En este caso, su administrador debe actualizar la política para permitirle acceso.

No estoy autorizado a realizar iam: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a Audit Manager.

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 Audit Manager. 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 AWS Audit Manager recursos

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 obtener información acerca de si Audit Manager admite estas características, consulte ¿Cómo AWS Audit Manager funciona 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.

Uso de funciones vinculadas a servicios para AWS Audit Manager

AWS Audit Manager utiliza funciones vinculadas al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Audit Manager. Audit Manager predefine las funciones vinculadas al servicio e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración AWS Audit Manager , ya que no es necesario añadir manualmente los permisos necesarios. Audit Manager define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Audit Manager puede asumir sus roles. 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.

Para obtener información sobre otros servicios que admiten roles vinculados al servicio, consulte Servicios deAWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado al servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de rol vinculado al servicio para AWS Audit Manager

Audit Manager usa el rol vinculado al servicio denominado**`AWSServiceRoleForAuditManager`**, que permite el acceso a los servicios y recursos de AWS utilizados o administrados por. AWS Audit Manager

El rol vinculado a servicios `AWSServiceRoleForAuditManager` confía en el servicio `auditmanager.amazonaws.com` para asumir el rol.

La política de permisos de funciones permite a Audit Manager recopilar pruebas automatizadas sobre su AWS uso. `AWSAuditManagerServiceRolePolicy` Más específicamente, puede tomar las siguientes acciones en su nombre.

- Audit Manager se puede utilizar AWS Security Hub para recopilar pruebas de verificación de conformidad. En este caso, Audit Manager utiliza el siguiente permiso para informar de los resultados de las comprobaciones de seguridad directamente desde AWS Security Hub. A continuación, adjunta los resultados a los controles de evaluación pertinentes como evidencia.
  - `securityhub:DescribeStandards`

  > **Note**
  >
  > Para obtener más información sobre qué controles específicos de Security Hub puede describir Audit Manager, consulte los controlesAWS Security Hub compatibles con AWS Audit Manager.

- Audit Manager se puede utilizar AWS Config para recopilar pruebas de verificación de conformidad. En este caso, Audit Manager utiliza los siguientes permisos para informar de los resultados de las evaluaciones de AWS Config reglas directamente desde AWS Config. A continuación, adjunta los resultados a los controles de evaluación pertinentes como evidencia.
  - `config:DescribeConfigRules`
  - `config:DescribeDeliveryChannels`
  - `config:ListDiscoveredResources`

  > **Note**
  >
  > Para obtener más información sobre qué AWS Config reglas específicas puede describir Audit Manager, consulte AWS Config Reglas compatibles con AWS Audit Manager.

- Audit Manager se puede utilizar AWS CloudTrail para recopilar pruebas de la actividad del usuario. En este caso, Audit Manager utiliza los siguientes permisos para capturar la actividad del usuario en CloudTrail los registros. A continuación, adjunta la actividad de los controles de evaluación pertinentes como evidencia.
  - `cloudtrail:DescribeTrails`
  - `cloudtrail:LookupEvents`

  > **Note**
  >
  > Para obtener más información sobre qué CloudTrail eventos específicos puede describir Audit Manager, consulte los nombres deAWS CloudTrail eventos compatibles con AWS Audit Manager.

- Audit Manager puede utilizar las llamadas a la AWS API para recopilar pruebas de configuración de recursos. En este caso, Audit Manager utiliza los siguientes permisos para llamar a las API de solo lectura que describen las configuraciones de sus recursos para los siguientes Servicios de AWS. A continuación, adjunta las respuestas de la API a los controles de evaluación pertinentes como evidencia.
  - `acm:GetAccountConfiguration`
  - `acm:ListCertificates`
  - `backup:ListRecoveryPointsByResource`
  - `bedrock:GetCustomModel`
  - `bedrock:GetFoundationModel`
  - `bedrock:GetModelCustomizationJob`
  - `bedrock:GetModelInvocationLoggingConfiguration`
  - `bedrock:ListCustomModels`
  - `bedrock:ListFoundationModels`
  - `bedrock:ListModelCustomizationJobs`
  - `cloudwatch:DescribeAlarms`
  - `cloudwatch:DescribeAlarmsForMetric`
  - `cloudwatch:GetMetricStatistics`
  - `cloudwatch:ListMetrics`
  - `cognito-idp:DescribeUserPool`

- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeTable
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters

- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport

- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents

- `organizations:DescribeOrganization`
- `organizations:DescribePolicy`
- `rds:DescribeCertificates`
- `rds:DescribeDbClusterEndpoints`
- `rds:DescribeDbClusterParameterGroups`
- `rds:DescribeDbClusters`
- `rds:DescribeDBInstances`
- `rds:DescribeDbSecurityGroups`
- `redshift:DescribeClusters`
- `route53:GetQueryLoggingConfig`
- `s3:GetBucketPolicy`
  - Esta acción de la API se lleva a cabo dentro del ámbito Cuenta de AWS en el service-linked-role que esté disponible. No puede acceder a las políticas de bucket entre cuentas.
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketVersioning`
- `s3:GetEncryptionConfiguration`
- `s3:GetLifecycleConfiguration`
- `s3:ListAllMyBuckets`
- `sns:ListTopics`
- `sqs:ListQueues`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:ListRuleGroups`
- `waf-regional:ListSubscribedRuleGroups`
- `waf-regional:ListWebACLs`
- `waf:ListActivatedRulesInRuleGroup`

> **Note**
>
> Para obtener más información sobre las llamadas a la API específicas que Audit Manager puede describir, consulte Se admiten llamadas a la API para orígenes de datos de control personalizadas.

Para ver todos los detalles de los permisos de la función vinculada al servicio`AWSServiceRoleForAuditManager`, consulta la Guía AWSAuditManagerServiceRolePolicyde referencia sobre políticasAWS gestionadas.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o 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.

Crear el rol vinculado al servicio AWS Audit Manager

No necesita crear manualmente un rol vinculado a servicios. Cuando lo habilitas AWS Audit Manager, el servicio crea automáticamente el rol vinculado al servicio por ti. Puede activar Audit Manager desde la página de incorporación de AWS Management Console, o mediante la API o AWS CLI. Para obtener más información, consulte Habilitar AWS Audit Manager en este guía del usuario.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta.

Edición del rol vinculado al AWS Audit Manager servicio

AWS Audit Manager no permite editar el rol vinculado al `AWSServiceRoleForAuditManager` servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol utilizando IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Permitir a una entidad de IAM editar la descripción del rol vinculado a servicio **`AWSServiceRoleForAuditManager`**

Agregue la siguiente instrucción a la política de permisos de la entidad de IAM que tiene que editar la descripción del rol vinculado al servicio.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "auditmanager.amazonaws.com"}}
```

```
}
```

Eliminar el rol vinculado al servicio AWS Audit Manager

Si ya no utiliza Audit Manager, le recomendamos que elimine el rol vinculado a servicios `AWSServiceRoleForAuditManager`. De esta forma, no tendrá una entidad no utilizada cuya supervisión o mantenimiento no se realizan de forma activa. Sin embargo, debe limpiar el rol vinculado al servicio antes de eliminarlo.

Limpieza del rol vinculado al servicio de

Antes de poder utilizar IAM para eliminar el rol vinculado a un servicio de Audit Manager, primero debe confirmar que dicho rol no tiene sesiones activas y eliminar los recursos que utiliza. Para ello, asegúrese de que Audit Manager esté dado de baja en todos los registros. Regiones de AWSTras anular el registro, Audit Manager ya no utiliza el rol vinculado al servicio.

Para obtener instrucciones sobre cómo anular el registro de Audit Manager, consulte los siguientes recursos:

- Desactivar AWS Audit Manager en esta guía
- DeregisterAccount en la Referencia de la API deAWS Audit Manager
- anular el registro de la cuenta en la referencia deAWS CLI AWS Audit Manager

Para obtener instrucciones sobre cómo eliminar los recursos de Audit Manager manualmente, consulte Eliminación de datos de Audit Manager en esta guía.

Eliminación del rol vinculado a un servicio

Puede eliminar el rol vinculado al servicio utilizando la consola de IAM, la AWS Command Line Interface (AWS CLI) o la API de IAM.

IAM console

Siga estos pasos para eliminar un rol vinculado en la consola de IAM.

Para eliminar un rol vinculado a un servicio (consola)

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 Roles. A continuación, maqrue la casilla de verificación situada junto a `AWSServiceRoleForAuditManager`, no el nombre o la propia fila.
3. En Acciones de rol en la parte superior de la página, elija Eliminar.
4. En el cuadro de diálogo de confirmación, revise la información de acceso reciente, donde se indica cuándo accedió cada uno de los roles seleccionados a un servicio de Servicio de AWSpor última vez. Esto lo ayuda a confirmar si el rol está actualmente activo. Si desea continuar, introduzca **`AWSServiceRoleForAuditManager`** en el campo de entrada de texto y seleccione Eliminar para enviar la solicitud de eliminación del rol vinculado al servicio.
5. Consulte las notificaciones de la consola de IAM para monitorear el progreso de la eliminación del rol vinculado al servicio. Como el proceso de eliminación del rol vinculado al servicio de IAM es asíncrono, dicha tarea puede realizarse correctamente o fallar después de que envía la solicitud de eliminación. Si el proceso se realiza correctamente, el rol se elimina de la lista y aparece un mensaje de confirmación en la parte superior de la página.

AWS CLI

Puede utilizar los comandos de IAM desde el AWS CLI para eliminar un rol vinculado a un servicio.

Para eliminar un rol vinculado a un servicio (AWS CLI)

1. Introduzca el siguiente comando para enumerar el rol de su cuenta:

```
aws iam get-role --role-name AWSServiceRoleForAuditManager
```

2. Como los roles vinculados a servicios no se puede eliminar si están en uso o tienen recursos asociados, debe enviar una solicitud de eliminación. Esta solicitud puede denegarse si no se cumplen estas condiciones. Debe apuntar el valor `deletion-task-id` de la respuesta para comprobar el estado de la tarea de eliminación.

   Ingrese el siguiente comando para enviar una solicitud de eliminación de un rol vinculado a un servicio:

```
aws iam delete-service-linked-role --role-name AWSServiceRoleForAuditManager
```

3. Utilice el siguiente comando para comprobar el estado de la tarea de eliminación:

```
aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```

El estado de la tarea de eliminación puede ser `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED` o `FAILED`. Si ocurre un error durante la eliminación, la llamada devuelve el motivo del error para que pueda resolver el problema.

IAM API

Puede utilizar la API de IAM para eliminar un rol vinculado a un servicio.

Para eliminar un rol vinculado a un servicio (API)

1. Llame GetRolepara incluir el rol en su cuenta. En la solicitud, especifique que `AWSServiceRoleForAuditManager` es el `RoleName`.
2. Como los roles vinculados a servicios no se puede eliminar si están en uso o tienen recursos asociados, debe enviar una solicitud de eliminación. Esta solicitud puede denegarse si no se cumplen estas condiciones. Debe apuntar el valor `DeletionTaskId` de la respuesta para comprobar el estado de la tarea de eliminación.

   Para enviar una solicitud de eliminación de un rol vinculado a un servicio, llame a DeleteServiceLinkedRole. En la solicitud, especifique que `AWSServiceRoleForAuditManager` es el `RoleName`.
3. Para comprobar el estado de la tarea de eliminación, realice una llamada a GetServiceLinkedRoleDeletionStatus. En la solicitud, especifique el valor de `DeletionTaskId`.

   El estado de la tarea de eliminación puede ser `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED` o `FAILED`. Si ocurre un error durante la eliminación, la llamada devuelve el motivo del error para que pueda resolver el problema.

> **Tip**
>
> La eliminación no se realiza correctamente si el servicio Audit Manager utiliza el rol o tiene recursos asociados. Esto solo ocurre si todavía está registrado en Audit Manager en uno o

más Regiones de AWS. Tras anular el registro, Audit Manager ya no utiliza el rol vinculado al servicio.
Para resolver un problema de eliminación fallida, primero asegúrese de anular el registro de Audit Manager en todos los Regiones de AWS lugares en los que utilizó el servicio. A continuación, vuelva a intentar seguir los pasos del procedimiento anterior.

Regiones compatibles para funciones vinculadas al servicio AWS Audit Manager

AWS Audit Manager admite el uso de funciones vinculadas al servicio en todos los lugares en los que el servicio Regiones de AWS esté disponible. Para obtener más información, consulte puntos de conexión de servicio deAWS.

Validación de conformidad para AWS Audit Manager

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimientoServicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > ProgramasAWS .

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: este documento técnico describe cómo las empresas pueden crear aplicaciones aptas para AWS 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 la perspectiva 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 paraAWS 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 AWS Audit Manager

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones 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.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura global.AWS

Seguridad de la infraestructura en AWS Audit Manager

Como servicio gestionado, AWS Audit Manager 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 SeguridadAWS 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.

Utilice las llamadas a la API AWS publicadas para acceder a AWS Audit Manager 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.

Puede llamar a estas operaciones de API desde cualquier ubicación de la red, pero AWS Audit Manager admite políticas de acceso basadas en los recursos, que pueden incluir restricciones basadas en la dirección IP de origen. También puede utilizar políticas de Audit Manager para controlar el acceso desde puntos de enlace específicos de Amazon Virtual Private Cloud (Amazon VPC) o VPC específicas. En efecto, esto aísla el acceso de red a un recurso de Audit Manager determinado únicamente de la VPC específica de la red. AWS

AWS Audit Manager y puntos finales de VPC de interfaz ()AWS PrivateLink

Puede establecer una conexión privada entre su VPC y crear un punto final AWS Audit Manager de VPC de interfaz. Los puntos de conexión de interfaz cuentan con tecnología de AWS PrivateLink que le permite acceder de forma privada a las API de Audit Manager sin una puerta de enlace de Internet, un dispositivo NAT, una conexión de VPN o una conexión de AWS Direct Connect. Las instancias de la VPC no necesitan direcciones IP públicas para comunicarse con las API de Audit Manager. El tráfico entre su VPC y AWS Audit Manager no sale de la AWS red.

Cada punto de conexión de la interfaz está representado por una o más interfaces de red elásticas en las subredes.

Para obtener más información, consulte Puntos de conexión de VPC de interfaz (AWS PrivateLink) en la Guía del usuario de Amazon VPC.

Consideraciones sobre los puntos AWS Audit Manager finales de VPC

Antes de configurar un punto de enlace de VPC de interfaz AWS Audit Manager, asegúrese de revisar las propiedades y limitaciones del punto de enlace de interfaz en la Guía del usuario de Amazon VPC.

AWS Audit Manager admite realizar llamadas a todas sus acciones de API desde su VPC.

Creación de un punto de conexión de VPC de interfaz para AWS Audit Manager

Puede crear un punto de enlace de VPC para el AWS Audit Manager servicio mediante la consola de Amazon VPC o el (). AWS Command Line Interface AWS CLIPara más información, consulte Creación de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Cree un punto final de VPC para AWS Audit Manager usar el siguiente nombre de servicio:

- `com.amazonaws.region.auditmanager`

Si habilitas el DNS privado para el punto final, puedes realizar solicitudes a la API para AWS Audit Manager utilizar su nombre de DNS predeterminado para la región, por ejemplo. `auditmanager.us-east-1.amazonaws.com`

Para más información, consulte Acceso a un servicio a través de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Crear una política de puntos de conexión de VPC para AWS Audit Manager

Puede asociar una política de punto de conexión con su punto de conexión de VPC que controla el acceso a AWS Audit Manager. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para más información, consulte Control del acceso a los servicios con puntos de enlace de la VPC en la Guía del usuario de Amazon VPC.

Ejemplo: política de puntos finales de VPC para acciones AWS Audit Manager

El siguiente es un ejemplo de una política de puntos finales para AWS Audit Manager. Cuando se asocia con un punto de conexión, esta política concede acceso a las acciones de Audit Manager mostradas para todas las entidades principales en todos los recursos.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "auditmanager:GetAssessments",
            "auditmanager:GetServicesInScope",
            "auditmanager:ListNotifications"
         ],
         "Resource":"*"
      }
   ]
}
```

Inicio de sesión y supervisión AWS Audit Manager

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Audit Manager y sus demás AWS soluciones. AWS proporciona las siguientes herramientas de supervisión para vigilar Audit Manager, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- AWS CloudTrail captura las llamadas a la API y otros eventos relacionados que realiza la Cuenta de AWS o que se realizan en nombre de esta. Además, entrega los archivos de registro a un bucket de Amazon S3 especificado. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que estas se realizaron. Para más información, consulte la Guía del usuario deAWS CloudTrail.
- 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 monitorear los eventos que ocurren en

los servicios y crear arquitecturas basadas en eventos. Para obtener más información, consulta la Guía del EventBridge usuario de Amazon.

Monitorización AWS Audit Manager con Amazon EventBridge

Amazon le EventBridge ayuda a automatizar los eventos del sistema Servicios de AWS y a responder automáticamente a ellos, como problemas de disponibilidad de las aplicaciones o cambios en los recursos.

Puede usar EventBridge reglas para detectar eventos de Audit Manager y reaccionar ante ellos. Según las reglas que cree, EventBridge invoca una o más acciones objetivo cuando un evento coincide con los valores que especifique en una regla. Dependiendo del tipo de evento, es posible que desee enviar notificaciones, capturar información sobre el evento, tomar medidas correctivas, iniciar eventos o adoptar otras acciones.

Por ejemplo: puede detectar cada vez que se produzcan los siguientes eventos de Audit Manager en su cuenta:

- El propietario de una auditoría crea, actualiza o elimina una evaluación
- El propietario de la auditoría delega un conjunto de controles para su revisión
- Un delegado completa su revisión y devuelve el conjunto de controles revisado al propietario de la auditoría
- El propietario de la auditoría actualiza el estado de un control de evaluación

Entre las acciones que se pueden activar automáticamente se incluyen las siguientes:

- Usa una AWS Lambda función para pasar una notificación a un canal de Slack.
- Envíe datos acerca de la verificación a un Amazon Kinesis Data Streams para permitir una supervisión completa y en tiempo real del estado.
- Envía un tema de Amazon Simple Notification Service (Amazon SNS) a su correo electrónico.
- Recibe una notificación con una acción de CloudWatch alarma de Amazon.

> **Note**
>
> Audit Manager ofrece eventos de forma duradera. Esto significa que Audit Manager intentará enviar eventos correctamente al EventBridge menos una vez. En los casos en los que los

eventos no se puedan entregar debido a una interrupción del EventBridge servicio, Audit Manager los volverá a intentar más adelante durante un máximo de 24 horas.

EventBridge formato de ejemplo para Audit Manager

El siguiente código JSON muestra un ejemplo de un evento de creación de una evaluación en Audit Manager. Para obtener información sobre cualquiera de los campos de este evento, consulte la referencia de la estructura del evento.

```
{
    "version": "0",
    "id": "55c5a6f3-6183-3989-49ec-a3c998857644",
    "detail-type": "Assessment Created",
    "source": "aws.auditmanager",
    "account": "111122223333",
    "time": "2023-07-27T00:38:33Z",
    "region": "us-west-2",
    "resources":
        [
            "arn:aws:auditmanager:us-west-2:111122223333:assessment/a1b2c3d4-e5f6-g7h8-
i9j0-k1l2m3n4o5p6"
        ],
    "detail":
    {
        "eventID": "4e939b2f-9429-3141-beec-d640d83ef68e",
        "author": "arn:aws:sts::111122223333:assumed-role/roleName/role-session-name",
        "assessmentTenantId": "111122223333",
        "assessmentName": "myAssessment",
        "eventTime": 1690418289068,
        "eventName": "CREATE",
        "eventType": "ASSESSMENT",
        "assessmentID": "a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"
    }
}
```

Requisitos previos para crear una regla EventBridge

Antes de crear reglas para los eventos de Audit Manager, recomendamos que haga lo siguiente:

- Familiarícese con los eventos, las reglas y los objetivos en EventBridge. Para obtener más información, consulta ¿Qué es Amazon EventBridge? en la Guía del EventBridge usuario de Amazon.
- Crear un destino que se va a usar en su regla de eventos. Por ejemplo: puede crear un tema de Amazon SNS de modo que cada vez que se complete una revisión de un conjunto de controles, reciba un mensaje de texto o un correo electrónico. Para obtener más información, consulta EventBridge los objetivos.

Creación de una EventBridge regla para Audit Manager

Siga estos pasos para crear una EventBridge regla que se active en un evento emitido por Audit Manager. Los eventos se emiten en la medida de lo posible.

Para crear una EventBridge regla para Audit Manager

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. En el panel de navegación, seleccione Reglas.
3. Seleccione Crear regla.
4. En la página Crear detalles de la regla, ingrese un nombre y una descripción para la regla.
5. Mantenga los valores predeterminados para Event bus (Bus de eventos) y Rules type (Tipo de regla) y luego seleccione Next (Siguiente).
6. En la página Crear un patrón de eventos, en Origen del evento, selecciona AWS eventos o eventos EventBridge asociados.
7. En Método de creación, elija Patrón personalizado (editor JSON).
8. En Patrón de eventos, escriba un patrón de eventos en JSON y especifique los campos que quiere usar para hacer coincidir.

   Para que coincida con un evento de Audit Manager, puede utilizar el siguiente patrón simple:

   ```
   {
     "detail-type": ["Event"]
   }
   ```

   Sustituya el *evento* por uno de los siguientes valores admitidos:

   a. Introduzca `Assessment Created` para recibir notificaciones cuando se cree una evaluación.

b. Introduzca `Assessment Updated` para recibir notificaciones cuando se cree una evaluación.

c. Introduzca `Assessment Deleted` para recibir notificaciones cuando se elimine una evaluación.

d. Introduzca `Assessment ControlSet Delegation Created` para recibir notificaciones cuando se delegue la revisión de un conjunto de controles.

e. Introduzca `Assessment ControlSet Reviewed` para recibir notificaciones cuando se revise un conjunto de control de evaluación.

f. Introduzca `Assessment Control Reviewed` para recibir notificaciones cuando se revise un control de evaluación.

> **Tip**
>
> Añada más campos a su patrón de eventos según sea necesario. Para obtener más información sobre los campos disponibles, consulta Amazon EventBridge Event Patterns.

9. Elija Siguiente.
10. En la página Seleccionar objetivos, elija el destino que haya creado para esta regla y, a continuación, configure las opciones adicionales necesarias para dicho tipo. Por ejemplo, si elige Amazon SNS, asegúrese de que el tema de SNS esté configurado correctamente para que se le notifique por correo electrónico o SMS.

> **Tip**
>
> Los campos que se muestran varían en función del servicio seleccionado. Para obtener más información sobre los objetivos disponibles, consulte Objetivos disponibles en la EventBridge consola.

11. Para muchos tipos de objetivos, EventBridge necesita permisos para enviar eventos al objetivo. En estos casos, EventBridge puede crear la función de IAM necesaria para que se ejecute la regla.

    a. Para crear un rol de IAM automáticamente, seleccione Crear un nuevo rol para este recurso específico.

    b. Para utilizar un rol de IAM que haya creado antes, elija Use existing role (Usar rol existente).

12. (Opcional) Elija Add another target (Agregar otro destino) para agregar otro destino para esta regla.
13. Seleccione Siguiente.
14. (Opcional) En la página Add tags (Agregar etiquetas) agregue etiquetas a su clave y, a continuación, elija Next (Siguiente).
15. En la página Review and create (Revisar y crear), revise la configuración de las reglas para asegurarse de que se ajustan a los requisitos de supervisión de eventos.
16. Elija Crear regla. Su regla se controlará ahora para eventos de Audit Manager y, a continuación, envíelos al destino que especificó.

Registrar las llamadas a AWS Audit Manager la API con CloudTrail

Audit Manager está integrado con CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un miembro Servicio de AWS de Audit Manager. CloudTrail captura todas las llamadas a la API de Audit Manager como eventos. Las llamadas que se capturan incluyen llamadas desde la consola de Audit Manager y llamadas de código a las operaciones de la API de Audit Manager.

Si crea un registro, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Audit Manager. Si no configura un registro, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos.

Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Audit Manager, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la GuíaAWS CloudTrail del usuario.

Información de Audit Manager en CloudTrail

CloudTrail está habilitada en su cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en Audit Manager, esa actividad se registra en un CloudTrail evento junto con otros Servicio de AWS eventos en el historial de eventos.

Puede ver, buscar y descargar los eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de eventos de CloudTrail .

Para obtener un registro continuo de los eventos de su Cuenta de AWSempresa, incluidos los eventos de Audit Manager, cree un registro. Un rastro permite CloudTrail entregar archivos de

registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique.

Además, puede configurar otros 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 más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail Integraciones y servicios compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de Audit Manager se registran CloudTrail y se documentan en la Referencia de laAWS Audit Manager API. Por ejemplo, las llamadas a las operaciones de la `CreateCustomControl` `UpdateAssessmentTemplate` API `DeleteControl` y a las operaciones de la API generan entradas en los archivos de CloudTrail registro.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

Para obtener más información, consulte el Elemento userIdentity de CloudTrail .

Descripción de las entradas del archivo de registros de Audit Manager

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud,

etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `CreateAssessment`acción.

```
{
      eventVersion:"1.05",
      userIdentity:{
        type:"IAMUser",
        principalId:"principalId",
        arn:"arn:aws:iam::accountId:user/userName",
        accountId:"111122223333",
        accessKeyId:"accessKeyId",
        userName:"userName",
        sessionContext:{
          sessionIssuer:{
          },
          webIdFederationData:{
          },
          attributes:{
            mfaAuthenticated:"false",
            creationDate:"2020-11-19T07:32:06Z"
          }
        }
      },
      eventTime:"2020-11-19T07:32:36Z",
      eventSource:"auditmanager.amazonaws.com",
      eventName:"CreateAssessment",
      awsRegion:"us-west-2",
      sourceIPAddress:"sourceIPAddress",
      userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
      requestParameters:{
        frameworkId:"frameworkId",
        assessmentReportsDestination:{
          destination:"***",
          destinationType:"S3"
        },
        clientToken:"***",
        scope:{
          awsServices:[
            {
```

```
            serviceName:"license-manager"
          }
        ],
        awsAccounts:"***"
      },
      roles:"***",
      name:"***",
      description:"***",
      tags:"***"
    },
    responseElements:{
      assessment:"***"
    },
    requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
    eventID:"a782029a-959e-4549-81df-9f6596775cb0",
    readOnly:false,
    eventType:"AwsApiCall",
    recipientAccountId:"recipientAccountId"
  }
```

Análisis de configuración y vulnerabilidad en AWS Audit Manager

La configuración y los controles de TI son una responsabilidad compartida entre usted AWS y usted, nuestro cliente. Para obtener más información, consulte el modelo de responsabilidad AWS compartida.

Etiquetado de recursos de AWS Audit Manager

Una etiqueta es un elemento de metadatos que usted o AWS asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor. En el caso de etiquetas que usted asigna, debe definir la clave y el valor. Por ejemplo, puede definir la clave como `stage` y el valor de un recurso como `test`.

Las etiquetas le ayudan a hacer lo siguiente:

- Localice fácilmente sus recursos de Audit Manager. Puede utilizar etiquetas como criterios de búsqueda al navegar por la biblioteca de marcos y la biblioteca de control.
- Asocie su recurso a un tipo de conformidad. Puede etiquetar varios recursos con una etiqueta específica de cumplimiento para asociar esos recursos a un marco específico.
- Identificar y organizar sus recursos de AWS. Muchos Servicios de AWS admiten el etiquetado, por lo que puede asignar la misma etiqueta a los recursos de diferentes servicios para indicar que los recursos están relacionados.
- Realizar un seguimiento de los costos de AWS. Estas etiquetas se activan en el panel de AWS Billing and Cost Management. AWS usa las etiquetas para clasificar los costos y enviar un informe mensual de asignación de costos. Para obtener más información, consulte Uso de etiquetas de asignación de costes en la Guía del usuario de AWS Billing and Cost Management.

En las siguientes secciones, se ofrece más información acerca de las etiquetas de AWS Audit Manager.

Recursos compatibles en Audit Manager

Los siguientes recursos de Audit Manager admiten el etiquetado:

- Evaluaciones
- Controles
- Marcos

Restricciones de las etiquetas

Las siguientes restricciones básicas se aplican a las etiquetas en los recursos de Audit Manager:

- Cantidad máxima de etiquetas que puede asignar a un recurso: 50

- Longitud máxima de la clave: 128 caracteres Unicode
- Longitud máxima del valor: 256 caracteres Unicode
- Caracteres válidos para claves y valores: a-z, A-Z, 0-9, espacio y los siguientes caracteres: _ . : / = + - y @
- Las claves y los valores distinguen entre mayúsculas y minúsculas
- No utilice `aws:` como prefijo para claves, ya que está reservado para AWS.

Administración de etiquetas

Puede configurar las etiquetas como propiedades al crear una evaluación, un marco o un control. Puede agregar, editar y eliminar etiquetas mediante la consola de Audit Manager, la AWS Command Line Interface (AWS CLI) y la API de Audit Manager. Para obtener más información, consulte los enlaces siguientes.

- Para las evaluaciones:
  - Creación de las evaluaciones y Edición de las evaluaciones en la sección Evaluaciones de esta guía
  - Pestaña de etiquetas en la sección Revisar una evaluación de esta guía
  - CreateAssessment y UpdateAssessment en la Referencia de AWS Audit Manager API
  - TagResource y UntagResource en la referencia de la API AWS Audit Manager
- Para los marcos:
  - Crear un marco personalizado y Editar un marco personalizado en la sección Bibliotecas de marcos de esta guía
  - En la pestaña Etiquetas de la sección Ver detalles del marco de esta guía
  - CreateAssessmentFramework y UpdateAssessmentFramework en la Referencia de AWS Audit Manager API
  - TagResource y UntagResource en la referencia de la API AWS Audit Manager
- Para controles:
  - Creación de un control personalizado y Editar un control personalizado en la sección Biblioteca de control de esta guía
  - Pestaña Etiquetas de la sección Ver detalles del control de esta guía
  - CreateControl y UpdateControl en la Referencia de AWS Audit Manager API
  - TagResource y UntagResource en la referencia de la API AWS Audit Manager

Creación de recursos de AWS Audit Manager con AWS CloudFormation

AWS Audit Manager está integrado con AWS CloudFormation, un servicio que le ayuda a modelar y configurar sus recursos de AWS para que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Puede crear una plantilla que describa todos los recursos de AWS que desea (por ejemplo, evaluaciones) AWS CloudFormation y aprovisiona y configura estos recursos por usted.

Cuando utiliza AWS CloudFormation, puede volver a utilizar la plantilla para configurar sus recursos de Audit Manager de forma coherente y repetida. Solo tiene que describir los recursos una vez y luego aprovisionar los mismos recursos una y otra vez en varias cuentas y regiones de AWS.

Audit Manager y plantillas AWS CloudFormation

Para aprovisionar y configurar los recursos de Audit Manager y sus servicios relacionados, debe entender las plantillas de AWS CloudFormation. Las plantillas son archivos de texto con formato de tipo JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus pilas de AWS CloudFormation. Si no está familiarizado con JSON o YAML, puede utilizar Designer de AWS CloudFormation para comenzar a utilizar las plantillas de AWS CloudFormation. Para obtener más información, consulte ¿Qué es AWS CloudFormation Designer? en la Guía del usuario de AWS CloudFormation.

Audit Manager admite la creación de evaluaciones en AWS CloudFormation. Para obtener más información, incluyendo ejemplos de plantillas JSON y YAML para las evaluaciones, consulte la referencia del tipo de recurso de AWS Audit Manager en la Guía del usuario de AWS CloudFormation.

Obtener más información sobre AWS CloudFormation

Para obtener más información acerca de AWS CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- Guía del usuario de AWS CloudFormation
- Referencia de la API de AWS CloudFormation
- Guía del usuario de la interfaz de la línea de comandos de AWS CloudFormation

Historial de revisión de la guía del usuario de AWS Audit Manager

En la siguiente tabla se describen los cambios importantes de cada versión de la Guía de usuario de AWS Audit Manager a partir del 8 de diciembre de 2020.

Cambio	Descripción	Fecha
Nuevo marco compatible: PCI DSS V4.0	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte PCI DSS V4.0.	19 de diciembre de 2023
Soporte para llamadas a AWS API adicionales	Ahora puede usar las llamadas a la AWS API adicionales como origen de datos para sus controles personalizados en Audit Manager. Para obtener más información, consulte Llamadas a la API compatibles para orígenes de datos de control personalizados.	7 de diciembre de 2023
Actualización de la política administrada AWS	AWS Audit Manager ha actualizado la AWSAuditManagerServiceRolePolicy. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	6 de diciembre de 2023
Soporte para resultados de control consolidados de AWS Security Hub	Audit Manager ahora admite controles consolidados en AWS Security Hub. Para	16 de noviembre de 2023

	obtener más información, consulte controles AWS Security Hub compatibles con AWS Audit Manager.	
Integración con MetricStream	Ahora puede incorporar evidencias de Audit Manager a MetricStream. Para obtener más información, consulte Integraciones con productos GRC de terceros.	14 de noviembre de 2023
Nuevo marco compatible: mejores prácticas de IA generativa de AWS	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte la versión 1 del marco de mejores prácticas de IA generativa de AWS.	8 de noviembre de 2023
Actualización de la política administrada AWS	AWS Audit Manager ha actualizado la AWSAuditManagerServiceRolePolicy. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	6 de noviembre de 2023
Integración con Amazon Eventbridge	Ahora puede supervisar los eventos que se producen en AWS Audit Manager y utilizarlos como parte de su arquitectura basada en eventos. Para más información, consulte Supervisión de AWS Audit Manager con Amazon EventBridge).	18 de agosto de 2023

Soporte para evaluaciones de riesgo y nuevas opciones de evidencias manuales	Ahora puede utilizar el flujo de trabajo de creación de controles personalizados para respaldar las evaluaciones de riesgos. Ahora, un control puede representar una pregunta de evaluación de riesgos y usted puede proporcionar una respuesta cargando un archivo o introduciendo texto como evidencia manual. Para obtener más información, consulte Crear un control personalizado y Añadir evidencia manual.	12 de junio de 2023
Soporte para exportaciones a CSV	Ahora puede exportar los resultados de búsqueda del buscador de evidencias en formato CSV. Para obtener más información, consulte Exportar resultados de búsqueda.	9 de junio de 2023
Nuevo marco compatible: Manual de seguridad de la información del Centro Australiano de Ciberseguridad (ACSC)	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte el Manual de seguridad de la información del Centro Australiano de Ciberseguridad (ACSC).	24 de marzo de 2023

Informes de evaluación mejorados	Hemos mejorado el formato y el contenido de los informes de evaluación de Audit Manager. Para obtener más información sobre cómo navegar e interpretar los informes de evaluació n, consulte Informes de evaluación.	23 de marzo de 2023
Soporte para llamadas a la API paginadas	AWS Audit Manager ahora admite las llamadas a la API paginadas como origen de datos para la recopilación de evidencias. Para obtener más información, consulte Llamadas a la API paginadas.	8 de marzo de 2023
Nuevo marco compatible: Regla de seguridad ómnibus final de la HIPAA de 2013	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte la Regla de seguridad ómnibus final de la HIPAA de 2013. Con fines de diferenciación, el marco HIPAA que existía anteriormente (anteriormente denominado HIPAA en la biblioteca de marcos) ahora se denomina Regla de seguridad de la HIPPA de 2003.	8 de marzo de 2023

Soporte para llamadas a AWS API adicionales	Ahora puede usar nueve llamadas a la AWS API adicionales como origen de datos para sus controles personalizados en Audit Manager. Para obtener más información, consulte Llamadas a la API compatibles para orígenes de datos de control personalizados.	3 de marzo de 2023
Guía actualizada para implementar las prácticas recomendadas de IAM	Se ha actualizado la guía para implementar las prácticas recomendadas de IAM. Para obtener más información, consulte prácticas recomendadas de seguridad en IAM.	6 de enero de 2023
Nueva configuración de retención de datos	Ahora puede especificar si desea eliminar todos sus datos al deshabilitar Audit Manager. Para obtener más información, consulte Deshabilitar AWS Audit Manager y Eliminar datos de Audit Manager.	6 de enero de 2023
Soporte para el buscador de evidencias	Ahora puede utilizar el buscador de evidencias para realizar consultas de búsqueda sobre los datos de las evidencias. Para obtener más información, consulte Buscador de evidencias.	18 de noviembre de 2022

Nuevo marco compatible: Australian Cyber Security Centre (ACSC) Essential Eight	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte Australian Cyber Security Centre (ACSC) Essential Eight.	24 de agosto de 2022
Actualización de la política administrada AWS	AWS Audit Manager ha actualizado la AWSAuditManagerServiceRolePolicy. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	7 de julio de 2022
Actualización de la política administrada AWS	AWS Audit Manager ha actualizado la AWSAuditManagerServiceRolePolicy. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	20 de mayo de 2022
Nuevo marco compatible: Canadian Centre for Cyber Security Medium Cloud Control Profile	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte Canadian Centre for Cyber Security Medium Cloud Control Profile.	6 de mayo de 2022

Actualización de la política administrada AWS	AWS Audit Manager ha actualizado la política de AWSAuditManagerAdministratorAccess. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	29 de abril de 2022
Soporte para reglas AWS Config administradas adicionales	Ahora puede utilizar 91 reglas administradas adicionales AWS Config como origen de datos para sus controles personalizados en Audit Manager. Para obtener más información, consulte Uso de reglas administradas AWS Config con AWS Audit Manager.	27 de abril de 2022
Soporte para reglas AWS Config personalizadas	Ahora puede usar reglas personalizadas de AWS Config como origen de datos para sus controles personalizados en Audit Manager. Para obtener más información, consulte Uso de reglas personalizadas AWS Config con AWS Audit Manager.	27 de abril de 2022
Nuevo marco compatible: ISO/IEC 27001:2013, anexo A	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte el Anexo A de la norma ISO/IEC 27001:2013.	7 de abril de 2022

Actualización de la política administrada AWS	AWS Audit Manager ha actualizado la AWSAuditManagerServiceRolePolicy. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	16 de marzo de 2022
Nuevos marcos compatibles: CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4	Ya están disponibles en AWS Audit Manager dos nuevos marcos prediseñados: CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4, nivel 1, y CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4, niveles 1 y 2. Para obtener más información, consulte CIS Benchmark para CIS AWS Audit Manager Foundations Benchmark v1.4.0.	2 de marzo de 2022
Nuevo marco compatible: CIS Controls v8 IG1	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte Controles CIS v8 IG1.	2 de marzo de 2022
Panel de AWS Audit Manager	Ahora puede utilizar el panel de control de Audit Manager para supervisar sus evaluaciones activas e identificar rápidamente las evidencias no conformes. Para obtener más información, consulte Uso del panel de Audit Manager.	18 de noviembre de 2021

Compartir un marco personalizado	Ahora puede compartir sus marcos personalizados de Audit Manager con otra Cuenta de AWS o replicarlos en otra Región de AWS con su propia cuenta. Para obtener más información, consulte Compartir un marco personalizado.	22 de octubre de 2021
Nuevos ejemplos de controles AWS Audit Manager	Ahora puede revisar ejemplos de controles y saber cómo Audit Manager ayuda a adaptar su entorno AWS a sus requisitos. Para obtener más información, consulte Ejemplos de controles AWS Audit Manager.	21 de septiembre de 2021
Nuevo marco compatible: Ley Gramm-Leach-Bliley (GLBA)	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte Ley Gramm-Leach-Bliley (GLBA).	2 de septiembre de 2021
Nuevo capítulo de solución de problemas	Ahora está disponible un nuevo capítulo de solución de problemas. Para más información, consulte Solución de problemas en AWS Audit Manager.	23 de agosto de 2021

Nuevo capítulo y tutorial sobre la delegación	Hemos ampliado la documentación de nuestra delegación en un nuevo capítulo. Para obtener más información, consulte Delegaciones en AWS Audit Manager. También hemos añadido un nuevo tutorial dirigido a los delegados que estén revisando un conjunto de controles por primera vez en AWS Audit Manager. Para obtener más informaci ón, consulte el Tutorial para delegados: Revisión de un conjunto de controles.	25 de junio de 2021
Nuevo marco compatible: NIST SP 800-171 Rev. 2	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte NIST SP 800-171 Rev. 2.	17 de junio de 2021
Informes de evaluación mejorados	Hemos mejorado el formato y el contenido de los informes de evaluación de AWS Audit Manager. Para obtener más información sobre cómo navegar y comprender los informes de evaluació n, consulte Informes de evaluación.	8 de junio de 2021

Página de nuevas políticas administradas por AWS	AWS Audit Manager ha comenzado el seguimiento de los cambios de las políticas administradas. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	6 de mayo de 2021
Nuevo marco compatible: Versión 1.1 del Marco de Ciberseguridad del NIST	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte la Versión 1.1 del Marco de Ciberseguridad del NIST.	5 de mayo de 2021
Nuevo marco compatible: AWS Well-Architected	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte AWS Well-Architected.	5 de mayo de 2021
Nuevo marco compatible: mejores prácticas básicas de seguridad de AWS	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte Prácticas recomendadas de seguridad básica de AWS.	5 de mayo de 2021
Nuevo marco compatible: GxP, anexo 11 de la UE	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte el GxP, anexo 11 de la UE.	28 de abril de 2021

Nuevo marco compatible: NIST 800-53 (Rev. 5) Bajo-Moderado-Alto	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte NIST 800-53 (Rev. 5) Bajo-Moderado-Alto.	25 de marzo de 2021
Nuevos marcos compatibles: CIS Benchmark para CIS Foundations Benchmark v1.3 AWS Audit Manager	Ahora hay disponibles dos nuevos marcos prediseñados en AWS Audit Manager: CIS Benchmark for CIS Foundations AWS Audit Manager Benchmark v1.3.0, nivel 1, y CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0, nivel 1 y 2. Para obtener más información, consulte CIS Benchmark para CIS AWS Audit Manager Foundations Benchmark v1.3.0.	22 de marzo de 2021
Versión inicial	Versión inicial de la Guía del usuario y Referencia de la API AWS Audit Manager.	8 de diciembre de 2020

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.